SonicWALL
Reporting Solutions

REPORTING | **SonicWALL ViewPoint**

SonicWALL ViewPoint 6.0 Administrator's Guide

SONICWALL®

SonicWALL ViewPoint Administrator's Guide

Version 6.0

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Copyright Notice

© 2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Windows XP, Windows Vista, Windows 7, Windows Server 2008, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Firefox is a trademark of the Mozilla Foundation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

End User Licensing Agreement For SonicWall ViewPoint

This End User Licensing Agreement (EULA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

The SOFTWARE PRODUCT is licensed, not sold.

You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

- The SOFTWARE PRODUCT is licensed as a single product and can only be used as such.
- You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network.
- You may not resell, or otherwise transfer for value, rent, lease, or lend the SOFTWARE PRODUCT.
- The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this EULA.
- You agree and certify that neither the SOFTWARE PRODUCT nor any other technical data received from SonicWALL, nor the direct product thereof, will be exported outside the United States except as permitted by

the laws and regulations of the United States, which may require U.S. Government export approval/licensing. Failure to strictly comply with this provision shall automatically invalidate this License.

License

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for a number of SonicWALL eligible products. This number is specified and shipped with the SOFTWARE PRODUCT. Support for additional SonicWALL eligible products is subject to a separate upgrade license.

Upgrades

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

Support Services

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT (“Support Services”). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in “online” documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this EULA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

Ownership

As between the parties, SonicWALL retains all title to, ownership of, and all proprietary rights with respect to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and ‘applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. The SOFTWARE PRODUCT is licensed, not sold. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

U.S. Government Restricted Rights

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government’s rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions. Contractor/Manufacturer is: SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124-3452, USA.

Exports License

Licensee will comply with, and will, at SonicWALL's request, demonstrate such compliance with all applicable export laws, restrictions, and regulations of the U.S. Department of Commerce, the U.S. Department of Treasury and any other any U.S. or foreign agency or authority. Licensee will not export or re-export, or allow the export or re-export of any product, technology or information it obtains or learns pursuant to this Agreement (or any direct product thereof) in violation of any such law, restriction or regulation, including, without limitation, export or re-export to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country subject to applicable U.S. trade embargoes or restrictions, or to any party on the U.S. Export Administration Table of Denial Orders or the U.S. Department of Treasury List of Specially Designated Nationals, or to any other prohibited destination or person pursuant to U.S. law, regulations or other provisions.

Miscellaneous

This EULA represents the entire agreement concerning the subject matter hereof between the parties and supercedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This EULA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this EULA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Termination

This EULA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this EULA if you fail to comply with the terms and conditions of this EULA. SonicWALL reserves the right to terminate this EULA five (5) years after the SOFTWARE PRODUCT is issued to Licensee. In event of termination, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

Limited Warranty

SonicWALL warrants that a) the software product will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of purchase, and b) any support services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the software product are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies

SonicWALL's and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

No Other Warranties

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Limitation of Liability

Except for the warranties provided hereunder, to the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any special, incidental, indirect, or consequential damages for lost business profits, business interruption, loss of business information,) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide support services, even if SonicWALL has been advised of the possibility of such damages. In any case, SonicWALL's entire liability under any provision of this EULA shall be limited to the amount actually paid by you for the SOFTWARE PRODUCT; provided, however, if you have entered into a SonicWALL support services agreement, SonicWALL's entire liability regarding support services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Manufacturer is SonicWALL, Inc. with headquarters located at 2001 Logic Drive, San Jose, CA 95124-3452, USA.

Table of Contents

Table of Contents **1**

Chapter 1: Introduction to SonicWALL ViewPoint **9**

SonicWALL ViewPoint Overview 9
SonicWALL ViewPoint Installation 10
License and Registration Requirements 10
Accessing the Correct Management Interface 11
Switching Between Management Interfaces 12
Tips and Tutorials 12
Navigating the ViewPoint User Interface 13
UTM Panel 13
SSL-VPN Panel 15
Console Panel 16
ViewPoint Views and Status 17
Using the ViewPoint TreeControl Menu 20
About Signed Applets in SonicWALL ViewPoint 21

Chapter 2: Using the UMH System Interface **23**

Overview of the UMH System Interface 24
Switching to the Application Interface 24
Viewing Online Help and Tips 24
Logging Out of the UMH System Interface 25
Configuring UMH System Settings 25
Viewing System Status 26
Managing System Licenses 26
Configuring System Administration Settings 28
Managing System Settings 29
Using System Diagnostics 30
Configuring UMH Deployment Options 31

Configuring the Deployment Role 32
Configuring Deployment Settings 34
Controlling Deployment Services 36

Chapter 3: Adding SonicWALL Appliances 37
Adding SonicWALL Appliances to SonicWALL ViewPoint 37
Adding SonicWALL Appliances 38
Modifying SonicWALL Appliance Settings 39
Deleting SonicWALL Appliances from ViewPoint 39

Chapter 4: Using the SonicToday Panel 41
Overview of the SonicToday Panel 42
Editing a Component Window 42
Adding a Component Window 44
Application Widget 44
RSS Feed 46
Adding More Pages 47
Editing and Deleting Pages 48
Other Features 49

Chapter 5: Configuring User Settings 51
Configuring General Settings 51
Configuring Reports Settings 53
Adding Web Sites to the Filter List 54
Deleting Web Sites from the Filter List 54
Adding Web Users to the Filter List 54
Deleting Web Users from the Filter List 55

Chapter 6: Configuring Log Settings 57
Configuration 57
View Log 58

Chapter 7: Configuring Management Settings 61
Settings 61
Configuring Email Settings 62
Configuring System Debug Level 62
Enforcing Password Security 63
Synchronizing Model Codes 63
Alert Settings 64
Sessions 65
Managing Sessions 65

Database Maintenance 66
Configuring Backup Schedule and Settings 67
Backing Up a Database Immediately 68
Restoring a Database Backup 68

Chapter 8: Managing Reports in the Console Panel 71
Settings 71
Enabling Report Table Sorting 72
Controlling the Number of Appliances with Log Viewer Enabled 72
Summarizer 73
About Summary Data in Reports 73
Summarizer Settings and Summarization Interval 73
Configuring the Syslog Deletion Schedule Settings 78
Configuring Host Name Resolution 79
Email / Archive 81
Configuring Email / Archive Settings 81
Scheduled Reports 82
Management 87
Configuring Report Data Management 87

Chapter 9: Using Diagnostics 89
Summarizer Status 90

Chapter 10: Granular Event Management 97
Granular Event Management Overview 97
What is Granular Event Management? 98
How Does Granular Event Management Work? 98
Using Granular Event Management 99
About Alerts 100
Configuring Granular Event Management 101
Configuring Events on the Console Panel 101
Enabling or Disabling Alerts on the UTM Panel 107
Viewing Current Alerts 108

Chapter 11: Web Services 109
URI Basics 110
Settings 111
Status 112

Chapter 12: Using ViewPoint Help 113
Tips and Tutorials 113

About ViewPoint 114

Chapter 13: ViewPoint Reporting Features 115

ViewPoint Reporting Overview 115
Viewing ViewPoint Reports 117
Navigating ViewPoint Reporting 119
Global Views 120
Unit View 121
Using Interactive Reports 122
Searching for a Report 123
Collapsible TreeControl Pane 128
Enabling/Disabling Scheduled Reports 128
Combined Reports 128
Improved Navigation 129
Showing Domain Names in Reports 130
Managing ViewPoint Reports on the Console Panel 131

Chapter 14: Scheduling and Configuring Reports 133

Configuring Scheduled Reports 134
Viewing or Managing Scheduled Reports 134
Adding or Editing a Scheduled Report 135
Selecting Reports for Summarization 137
Configuring Inheritance for Reporting Screens 138
Configuring Data Storage Settings 139
Configuring Summarization Data for Top Usage 140
Configuring Summarization Data for Bandwidth Reports 141
Configuring Dashboard Summary Reports 142
Viewing Current Alerts 144
Scheduling PDF Compliance Reports 144
Compliance Report Overview 144
Adding a New Scheduled Compliance Report 145
Customizing Your Detailed Reports Page 149

Chapter 15: Viewing Reports 153

Managing Report Settings 154
Editing Report Settings 154
Selecting a Graphical Display 154
Setting a Date or Date Range 155
Additional Settings 156
Troubleshooting Reports 156
Viewing General Status Reports 157

Viewing Dashboard Reports 159
Viewing the Dashboard Summary Report 159
Viewing the Security Dashboard Report 162
Using Custom Reports on UTM Appliances 163
Toggling Between Split Mode and Full Mode 164
Configuring the Date and Time for Custom Reports 166
Configuring the Report Layout and Generating the Report 168
Generating the Custom Report 176
Viewing a Custom Report 177
Printing a Page or Exporting the Report as a PDF or CSV File 179
Saving the Report Template 180
Viewing Bandwidth Reports 180
Viewing the Bandwidth Summary Report 181
Viewing the Top Users of Bandwidth 183
Viewing Bandwidth Usage Over Time 185
Viewing the Top Users of Bandwidth Over Time 187
Viewing Services Reports 189
Viewing the Services Summary Report 189
Viewing Web Usage Reports 191
Viewing the Web Usage Summary Report 192
Viewing the Top Web Sites 194
Viewing the Top Users of Web Bandwidth 195
Viewing Web Usage by User 197
Viewing Web Usage By Site 199
Viewing Web Usage By Category 200
Viewing Web Usage Over Time 202
Viewing Top Sites Over Time 203
Viewing Top Users Over Time 205
Viewing Web Usage By User Over Time 207
Viewing Web Usage By Category Over Time 208
Viewing Web Filter Reports 209
Viewing the Web Filter Summary Report 210
Viewing the Web Filter Top Sites Report 212
Viewing the Top Users that Try to Access Blocked Sites 213
Viewing the Blocked Sites for Each User 215
Viewing Blocked Sites Sorted By Site 216
Viewing Blocked Sites Sorted By Category 217
Viewing Blocked Site Attempts Over Time 219
Viewing the Top Blocked Site Attempts Over Time 220
Viewing the Top Blocked Site Users Over Time 221
Viewing Blocked Sites for Each User Over Time 222

Viewing Blocked Sites By Category Over Time 223
Viewing File Transfer Protocol Reports 225
Viewing the FTP Summary Report 225
Viewing the Top FTP Sites By User 227
Viewing FTP Bandwidth Usage Over Time 228
Viewing the Top Users of FTP Bandwidth Over Time 230
Viewing Mail Usage Reports 231
Viewing the Mail Usage Summary Report 232
Viewing the Top Users of Mail Bandwidth 234
Viewing Mail Usage Over Time 235
Viewing the Top Users of Mail Bandwidth Over Time 237
Viewing VPN Usage Reports 238
Viewing the VPN Usage Summary Report 239
Viewing the Top VPN Users 241
Viewing VPN Usage Over Time 242
Viewing the Top VPN Users Over Time 243
Viewing VPN Usage By Policy 245
Viewing the Top VPN Policies Over Time 246
Viewing Hourly VPN Usage By Policy 248
Viewing the VPN Services Summary Report 249
Viewing Attacks Reports 250
Viewing the Attack Summary Report 251
Viewing the Attacks By Category 253
Viewing the Errors Report 254
Viewing Attack Reports Over Time 256
Viewing the Attacks By Category Over Time 257
Viewing Errors Over Time 258
Viewing Virus Attacks Reports 260
Viewing the Top Viruses By Attack Attempts Report 262
Viewing the Virus Attack Attempts Report 263
Viewing the Virus Attacks By User Report 265
Viewing Anti-Spyware Reports 266
Viewing a Spyware Summary 268
Viewing Spyware Attempts By Category 269
Viewing Spyware Attempts Over Time 270
Viewing Spyware Attempts By Category Over Time 272
Viewing Intrusion Prevention Reports 273
Viewing the Intrusion Prevention Summary Report 275
Viewing Intrusion Attempts By Category 276
Viewing Intrusions Over Time 278
Viewing Intrusion Reports By Category Over Time 280

Viewing Application Firewall Reports 281
Viewing the Application Firewall Summary Report 282
Viewing the Application Firewall Over Time Report 283
Viewing Application Firewall Top Applications 284
Viewing Application Firewall Top Users 285
Viewing Application Firewall Top Policies 286
Viewing Authentication Reports 287
Viewing the User Login Report 288
Viewing the Administrator Login Report 289
Viewing the Failed Login Report 289
Viewing the Log 290
Viewing the Log for a SonicWALL Appliance 291

Chapter 16: SSL-VPN Reporting 293

SSL-VPN Reporting Overview 293
What is SSL-VPN Reporting? 294
Benefits of SSL-VPN Reporting 294
How Does SSL-VPN Reporting Work? 295
Using and Configuring SSL-VPN Reporting 295
About Viewing Available SSL-VPN Report Types 295
Configuring SSL-VPN Scheduled Reports 296
Configuring SSL-VPN Summarization 297

Chapter 17: Viewing SSL-VPN Reports 299

Viewing General Status Reports 299
Viewing SSL-VPN Bandwidth Reports 301
Viewing SSL-VPN Bandwidth Summary Reports 301
Viewing SSL-VPN Top Users of Bandwidth Reports 303
Viewing SSL-VPN Bandwidth Usage Over Time Reports 304
Viewing SSL-VPN Top Users of Bandwidth Over Time Reports 306
Using SSL-VPN Custom Reports 307
Toggling Between Split Mode and Full Mode 308
Configuring the Date and Time for Custom Reports 311
Configuring the Report Layout and Generating the Report 314
Generating the Custom Report 320
Viewing a Custom Report 321
Printing a Page or Exporting the Report as a PDF or CSV File 323
Saving the Report Template 324
Viewing SSL-VPN Resources Reports 325
Viewing SSL-VPN Resources Summary Reports 325
Viewing SSL-VPN Resources Top Users Reports 327

Viewing SSL-VPN Authentication Reports 330
Viewing SSL-VPN User Login Reports 330
Viewing SSL-VPN Failed Login Reports 331
Viewing the SSL-VPN Log 332
Viewing the Log for a SSL-VPN Appliance 332

Appendix A: Installing SonicWALL ViewPoint 335

About Installing and Upgrading SonicWALL ViewPoint 336
Installing SonicWALL ViewPoint 336
Installation Overview 336
Activating SonicWALL ViewPoint on Your Appliances 340
Registering Your SonicWALL Appliance 341
Activating the ViewPoint Software on Your Appliance 341
Enabling the ViewPoint License on Your Appliance 342
Installing Universal Management Suite 342
Upgrading SonicWALL ViewPoint 5.1 to 6.0 349
Registering SonicWALL ViewPoint 351
Configuring Deployment Settings 354
Configuring Web Port Settings 354
Configuring SMTP Settings 355
Upgrading from ViewPoint to GMS 356
Enabling the GMS Free Trial from ViewPoint 357
Enabling the GMS Free Trial from the UMH Interface 359
Completing the Free Trial Upgrade 360
Configuring Appliances for GMS Management 364
Purchasing a SonicWALL GMS Upgrade 366
Miscellaneous Procedures and Troubleshooting Tips 368
Miscellaneous Procedures 368
Troubleshooting Tips 370

Appendix B: Technical Tips 373

Log Viewer 373
Real-time Syslog Viewer 375
Forwarding Syslog Data to Another Syslog Server 376
Posting ViewPoint Reporting to Another Web Server for End-User Access 377

Index 379

CHAPTER 1
Introduction to SonicWALL ViewPoint

This chapter provides an overview of SonicWALL ViewPoint and information about the user interface.

See the following sections:

- "SonicWALL ViewPoint Overview" on page 9
- "SonicWALL ViewPoint Installation" on page 10
- "Accessing the Correct Management Interface" on page 11
- "Navigating the ViewPoint User Interface" on page 13
- "ViewPoint Views and Status" on page 17
- "Using the ViewPoint TreeControl Menu" on page 20
- "About Signed Applets in SonicWALL ViewPoint" on page 21

SonicWALL ViewPoint Overview

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. SonicWALL ViewPoint Reporting complements SonicWALL's network security offerings by providing detailed and comprehensive reports of network activity.

TheViewPoint Reporting Module is a software application that creates dynamic, Web-based network reports. The ViewPoint Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWALL network security appliances. With ViewPoint Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs.

The ViewPoint Reporting Module:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site
- Provides detailed daily logs to analyze specific events.

SonicWALL ViewPoint Installation

SonicWALL ViewPoint can be installed as a fresh install or as an upgrade to SonicWALL ViewPoint 5.0 and above.

Beginning in SonicWALL ViewPoint 5.1, all software components related to SonicWALL ViewPoint and SonicWALL Global Management System (GMS), including the MySQL database, executable binary files for all services, and other necessary files, are installed using the Universal Management Suite (UMS) single-binary installer. All SonicWALL ViewPoint and SonicWALL GMS files are installed as part of the Universal Management Suite, but no distinction is made between SonicWALL ViewPoint and SonicWALL GMS during the installation. The initial installation phase takes just a few minutes for any type of installation, such as a SonicWALL ViewPoint server, a SonicWALL GMS server, a database server, or any other role.

To install the Universal Management Suite from the single binary installer, see the "Installing Universal Management Suite" section on page 342.

License and Registration Requirements

SonicWALL ViewPoint is registered and licensed from the Windows server on which it is installed. SonicWALL ViewPoint registration is performed using the SonicWALL Universal Management Host system interface.The "Registering SonicWALL ViewPoint" section on page 351 provides detailed instructions for registering and licensing SonicWALL ViewPoint on your Windows system.

On SonicWALL appliances that send reporting data to SonicWALL ViewPoint, ViewPoint is licensed and activated separately from SonicOS. MySonicWALL provides a way to associate SonicWALL appliances with the SonicWALL ViewPoint instance installed on the Windows system. Licensing your SonicWALL ViewPoint application on a SonicWALL appliance requires:

- **A MySonicWALL account**. A MySonicWALL account allows you to manage your SonicWALL products and purchase licenses for various services. Creating a MySonicWALL account is fast, simple, and free. Simply complete an online registration form directly from your SonicWALL security appliance management interface. Your MySonicWALL account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser. Once you have an account, you can purchase SonicWALL ViewPoint and other licenses for your registered SonicWALL security appliances.
- **A registered SonicWALL security appliance with active Internet connection**. You need to register your SonicWALL security appliance to activate SonicWALL ViewPoint. Registering your SonicWALL security appliance is a simple procedure done directly from the management interface. Once your SonicWALL security appliance is registered, you can activate SonicWALL ViewPoint by using an activation key or by synchronizing with mysonicwall.com.

Accessing the Correct Management Interface

SonicWALL ViewPoint includes two separate management interfaces:

- **SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the SonicWALL ViewPoint instance, including registration and licensing, setting the admin password, creating backups, restarting the system, configuring network settings, selecting the deployment role, and configuring other system settings.
  Access the system management interface with the URL:

  http://<IP address>:<port>/appliance/

  If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address. If you are accessing the interface from the same system on which it is installed, use the following URL:

  http://localhost/appliance/

- **SonicWALL ViewPoint Management Interface** – Used to access the SonicWALL ViewPoint application that runs on the system. This interface is used to configure and view SonicWALL ViewPoint reporting on SonicWALL appliances and for configuring SonicWALL ViewPoint administrative settings. Access the SonicWALL ViewPoint management interface with one of the following URLs:

  http://<IP address>:<port>/sgms/
  http://localhost/sgms/

Switching Between Management Interfaces

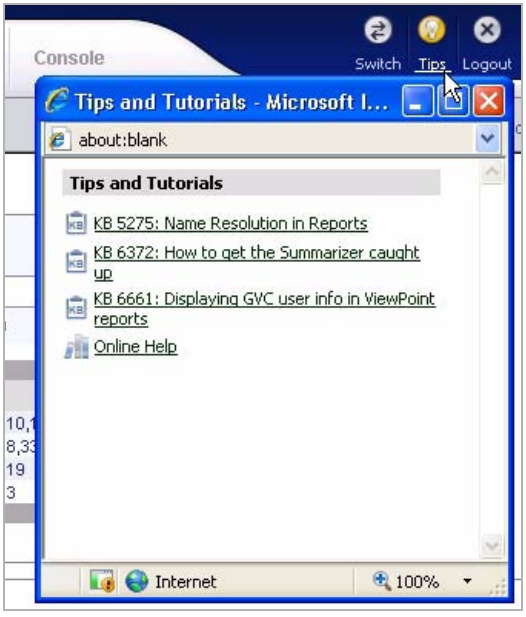
You can easily switch between the SonicWALL UMH system management interface and the SonicWALL ViewPoint application management interface.

One methods is to change the URL by adding **/sgms** for the ViewPoint application interface or adding **/appliance** for the UMH interface.

A second method involves clicking the **Switch** icon. While logged into either interface, you can switch to the login page of the other interface by clicking the **Switch** button in the top right corner of the page.

Tips and Tutorials

Tips and tutorials are also available in some section of the user interface, and are denoted by a “Lightbulb” icon:



To access tips and tutorials:

1. Navigate to the page where you need help.
2. If available, click the Lightbulb icon in the upper right-hand corner of the window. Tips, tutorials, and online help are displayed for this topic.

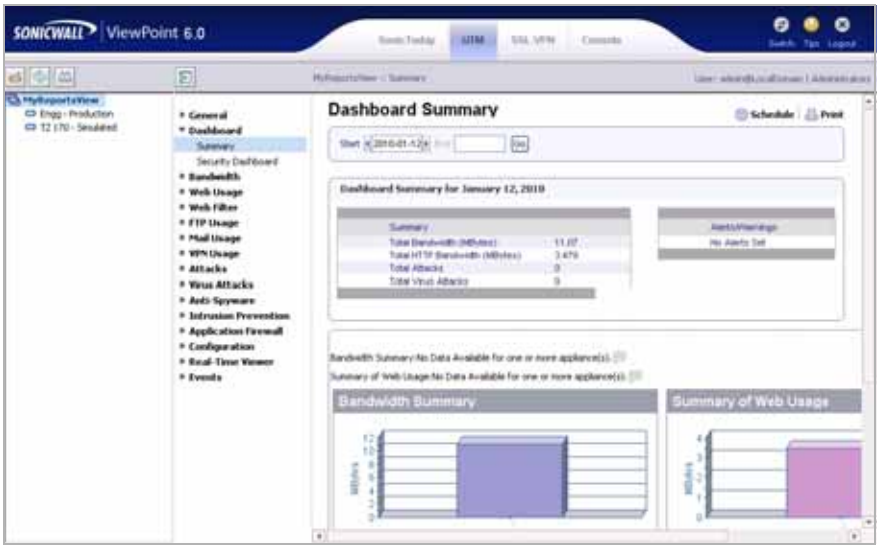
Navigating the ViewPoint User Interface

This section describes the UTM, SSL-VPN, and Console panels in the SonicWALL ViewPoint user interface. For information about the SonicToday panel, see the Using the SonicToday Panel chapter.

UTM Panel

The UTM Panel is an essential component of network security that is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

To open the UTM Panel, click the **UTM** tab at the top of the ViewPoint user interface.



From the UTM Panel, you can view the following for connected SonicWALL appliances:

- View general unit status, license status, and syslog settings.
- View the SonicWALL security dashboard. Dashboard reports display an overview of bandwidth, uptime, intrusions and attacks, and alerts for connected SonicWALL UTM appliances. The Security Dashboard report provides data about worldwide security threats that can affect your network. The Dashboard also displays data about threats blocked by the SonicWALL security appliance.

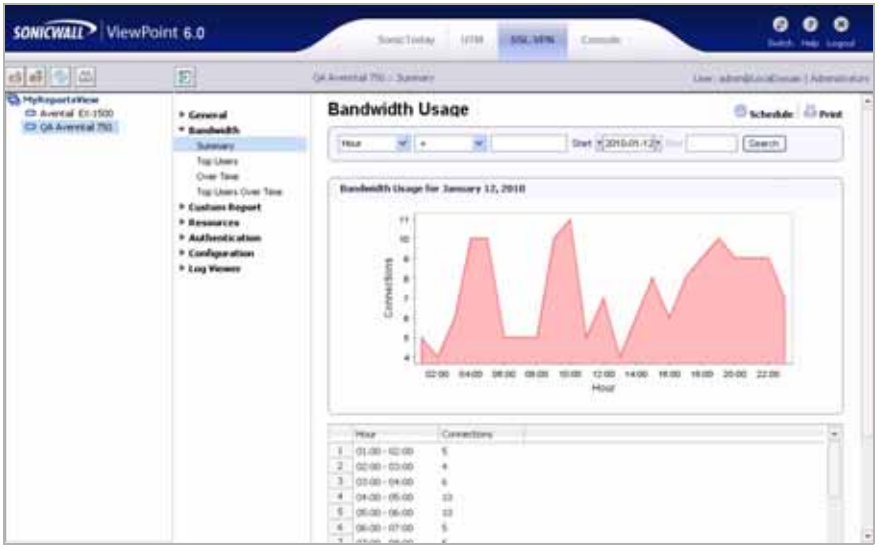
- View custom reports of Internet activity or Website filtering at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as “Week to date”. You can filter by user, domain, protocol, traffic, and full URL categories, depending on the type of custom report. The search template can be saved for use again later with the same appliance.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View a services report. This report includes information about events and usage of protocols and megabytes.
- View Web bandwidth usage. These reports include a daily bandwidth summary report, a top visited sites report, a top users of Web bandwidth report, a report that contains the top sites of each user, and a weekly summary report.
- View the number of attempts that users made to access blocked websites. These reports include a daily summary report, a top blocked sites report, a top users report, a report that contains the top blocked sites of each user, and a weekly summary report.
- View file transfer protocol (FTP) bandwidth usage. These reports include a daily FTP bandwidth summary report, a top users of FTP bandwidth report, and a weekly summary report.
- View mail bandwidth usage. These reports include a daily mail summary report, a top users of mail report, and a weekly summary report.
- View VPN usage. These reports include a daily VPN summary report, a top users of VPN bandwidth report, and a weekly summary report.
- View reports on attempted attacks and errors. The attack reports include a daily attack summary report, an attack by category report, a top sources of attacks report, and a weekly attack summary report. The error reports include a daily error summary report and a weekly error summary report.
- View reports on attempted virus attacks. Virus attacks reports are available for appliances that are licensed for SonicWALL Gateway Anti-Virus. These reports include the most frequent virus attack attempts, virus attacks by top destinations, virus attacks over time, virus attacks over a period of time, and virus attacks by top destinations over time.
- View reports on attempted spyware attacks. Anti-spyware reports are available for appliances that are licensed for SonicWALL Anti-Spyware. These reports include spyware attacks by category, spyware attacks over time, and spyware attacks by category over time.

- View reports on attempted intrusion attacks. Intrusion prevention reports are available for appliances that are licensed for SonicWALL Intrusion Prevention Service. These reports include intrusion attacks by source IP address, intrusion attacks by category, intrusion attacks over time, and intrusion attacks by category over time.
- View reports on traffic triggering Application Firewall policies. Application Firewall reports are available for UTM appliances that are licensed for SonicWALL Application Firewall. These reports include summary, over time, top applications, top users, and top policies.
- View successful and unsuccessful user and administrator authentication attempts. These reports include a user authentication report, an administrator authentication report, and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.
- View current alerts and access alert settings.

SSL-VPN Panel

The SSL-VPN panel provides access to SSL VPN appliances and is similar to the UTM panel. It is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

To open the SSL-VPN Panel, click the **SSL-VPN** tab at the top of the ViewPoint user interface.



From the SSL-VPN Panel, you can view the following for connected SonicWALL SSL VPN appliances:

- View general unit status, license status, and syslog settings.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View custom reports of custom reports of resource activity at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as “Week to date”. You can filter by user, protocol, destination IP, and source IP categories. The search template can be saved for use again later with the same appliance.
- View a resources report. This report includes information about connections and the resource used to connect, such as HTTPS or NetExtender.
- View successful and unsuccessful user authentication attempts. These reports include a user authentication report and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.

Console Panel

The Console Panel is used to configure SonicWALL ViewPoint settings, view pending tasks, view the log, manage licenses, and configure alerts.

To open the Console Panel, click the **Console** tab at the top of the SonicWALL ViewPoint user interface.

From the Console Panel, you can do the following:

- Change the SonicWALL ViewPoint password, adjust the amount of inactive time before the user is automatically logged out of ViewPoint, and set the maximum number of rows displayed on paginated screens.
- Configure Web sites and Web users that will be excluded from Web usage reports.
- View the SonicWALL ViewPoint log and delete old log messages. The SonicWALL ViewPoint log contains information on alert notifications, failed SonicWALL ViewPoint login attempts, and other events that apply to SonicWALL ViewPoint.
- Manage SMTP settings, system email addresses, archive report settings, debug level for logs, and password security settings. You can set the schedule and server settings, and the email alert recipient schedule and preferred format.
- Manage login sessions. You can view the status of user sessions and, if necessary, end them.
- Configure report settings for sort options and maximum units with Log Viewer enabled. Enabling Log Viewer allows custom reports for the system, but is resource intensive.
- Control summarizer settings, syslog and summarized data deletion schedules, and host name resolution settings.
- Configure email archive settings and search settings for scheduled reports, and manage data archiving.
- View summarizer diagnostics, useful for capacity planning.
- Configure granular event management report settings, including threshold, schedule, and alert settings.
- Configure Web services deployment settings and view Web services status.
- View the version number, serial number, and database information for SonicWALL ViewPoint, and access links to all available tips and video tutorials.

ViewPoint Views and Status

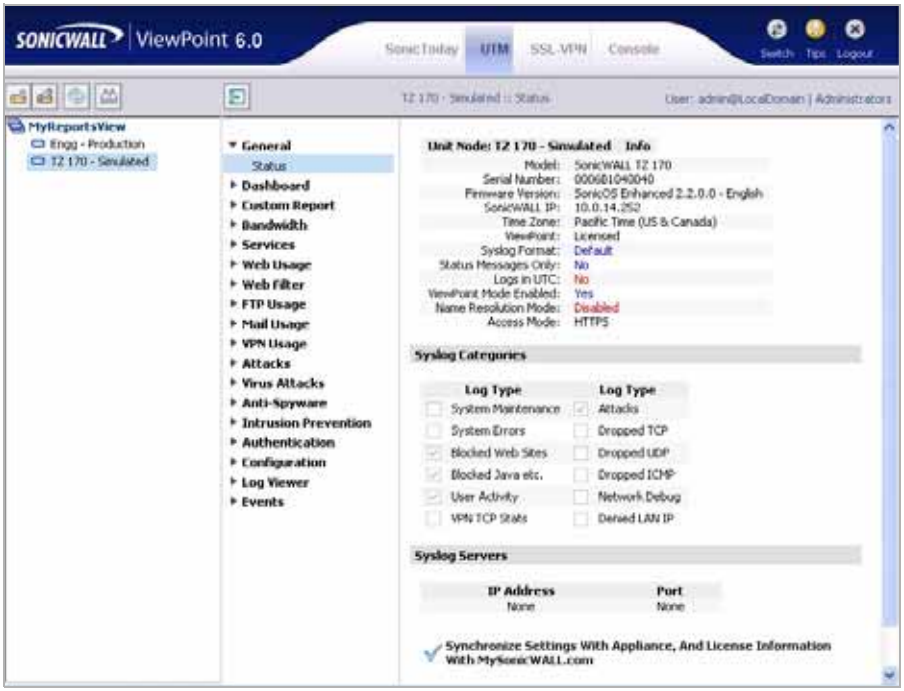
SonicWALL ViewPoint allows you to view status and reports for all appliances at once using **MyReportsView**, or for a single unit at a time with the **Unit** view.

ViewPoint provides status information on the General > Status page of the UTM or SSL-VPN panel.

MyReportsView is a grouping of all the appliances you are monitoring with ViewPoint. From the MyReportsView of the UTM or SSL-VPN Panel, Summary and Over Time reports are available for all SonicWALL appliances monitored by SonicWALL ViewPoint.

To open the My Reports view, click the **MyReportsView** icon at the top of the left pane. To display the global status page, navigate to **General > Status**.

From the Unit view, reports contain detailed data for the selected SonicWALL appliance. To specify the unit view, click any unit in the left pane. To display the unit status page, navigate to **General > Status** on the **UTM** or **SSL-VPN** panel.



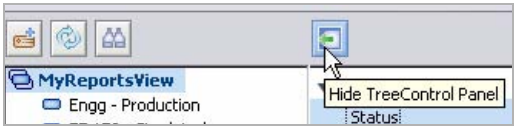
Using the ViewPoint TreeControl Menu

This section describes the content of the TreeControl menu within the SonicWALL ViewPoint user interface.

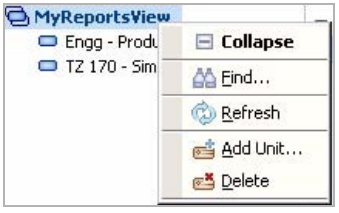
You can control the display of the TreeControl pane by selecting one of the appliance tabs at the top of the main window. For example, when you click the **UTM** tab, the TreeControl pane displays all the connected UTM appliance units. The two appliance tabs can display the following appliance types when ViewPoint is monitoring these device types:

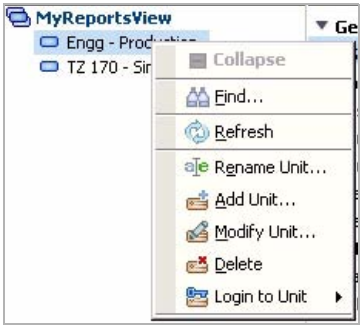
- UTM appliances
- SSL-VPN and EX-Series SRA appliances

You can hide the entire TreeControl pane by clicking the sideways arrow icon, and redisplay the pane by clicking it again. This is helpful when viewing some reports or other extra-wide screens.



To open a TreeControl appliance menu, right-click MyReportsView or a Unit icon.





The following options are available in the right-click menu:

- **Find** – Opens a Find dialog box that allows you to search for units.
- **Refresh** – Refreshes the ViewPoint UI display.
- **Rename Unit** – (unit view only) Renames the selected SonicWALL appliance.
- **Add Unit** – Add a new unit to the ViewPoint view. Requires unit IP and login information.
- **Modify Unit** – (unit view only) Change basic settings for the selected unit, including unit name, IP and login information, and serial number.

- **Delete** – Delete the selected unit
- **Login to Unit** – (unit view only) Login to the selected unit using HTTP or HTTPS protocols.

About Signed Applets in SonicWALL ViewPoint

There are a number of applets in the SonicWALL ViewPoint management interface, such as the TreeControl Applet in the leftmost pane.

Signed Applets refers to a technique for adding a digital signature to a Java applet to prove that it was not tampered with upon receipt from the signer. Signed applets can be given more privileges than ordinary applets. By default, applets have no access to system resources outside the directory from which they were launched, but a signed applet can access local system resources as allowed by the local system's security policy.

In some previous releases of ViewPoint, you were required to edit the java.policy file yourself on the client browser system in order to enable a number of applet related operations, such as Copy/Paste, Import file, Browse local folders, and HTTP/HTTPS login to the managed units from the ViewPoint management interface.

There is no need to edit the java.policy file for signed applets. When a signed applet starts up, a warning pop-up is displayed. If you want to trust the applet, click **Yes**. Copy/paste, Import and HTTP/HTTPS logins will work without any edits to the java.policy file.

Warning - Security
Do you want to trust the signed applet distributed by "SonicWALL Inc."?
Publisher authenticity verified by: "VeriSign, Inc."
The security certificate was issued by a company that is trusted.
The security certificate has not expired and is still valid.
Caution: "SonicWALL Inc." asserts that this content is safe. You should only accept this content if you trust "SonicWALL Inc." to make that assertion.
More Details
Yes
No
Always

Otherwise, click **No**. In this case you must manually edit the java.policy file. You can view the following technote for more information about editing the java.policy file:

Manually Configuring the java.policy File for SonicWALL GMS JRE

CHAPTER 2
Using the UMH System Interface

This chapter describes the Universal Management Host system interface, one of the two management interfaces available for SonicWALL ViewPoint.

This section includes the following subsections:

- Overview of the UMH System Interface, page 24
- Configuring UMH System Settings, page 25
- Configuring UMH Deployment Options, page 31

Overview of the UMH System Interface

The SonicWALL ViewPoint UMH system interface is used for system management of the SonicWALL ViewPoint instance, including registration and licensing, setting the admin password, configuring network and database settings, selecting the deployment role, and configuring other system settings.

When installing SonicWALL Universal Management Suite 6.0 on a host, a Web server is installed to provide the system management interface. The system interface is available by default at http://localhost/appliance/ after restarting the system.

Switching to the Application Interface

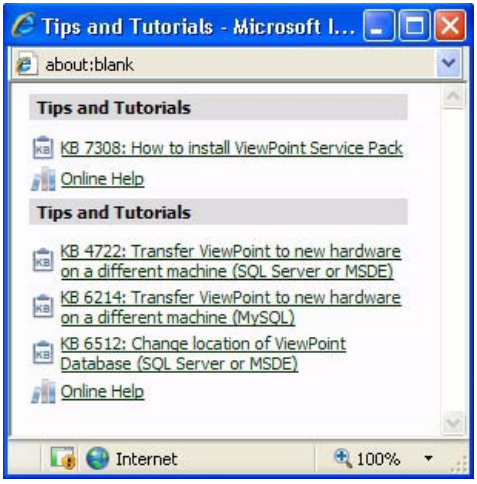
To switch between the System interface and the SonicWALL ViewPoint application interface, click the **Switch** button in the top right corner of the interface.

Viewing Online Help and Tips

To display context sensitive help for the current page, click the **Help** button in the top right corner of the interface.

The **Help** button can change to the **Tips** button if the current page has any context sensitive tips or video tutorials.

Clicking on the **Tips** button displays dynamic links for whitepapers, videos, knowledge base articles, other references, and online help.


Tips and Tutorials - Microsoft I...
about:blank
Tips and Tutorials
KB 7308: How to install ViewPoint Service Pack
Online Help
Tips and Tutorials
KB 4722: Transfer ViewPoint to new hardware on a different machine (SQL Server or MSDE)
KB 6214: Transfer ViewPoint to new hardware on a different machine (MySQL)
KB 6512: Change location of ViewPoint Database (SQL Server or MSDE)
Online Help
Internet
100%

Logging Out of the UMH System Interface

To log out of the SonicWALL ViewPoint UMH system interface, click the **Logout** button in the top right corner of the interface.

Configuring UMH System Settings

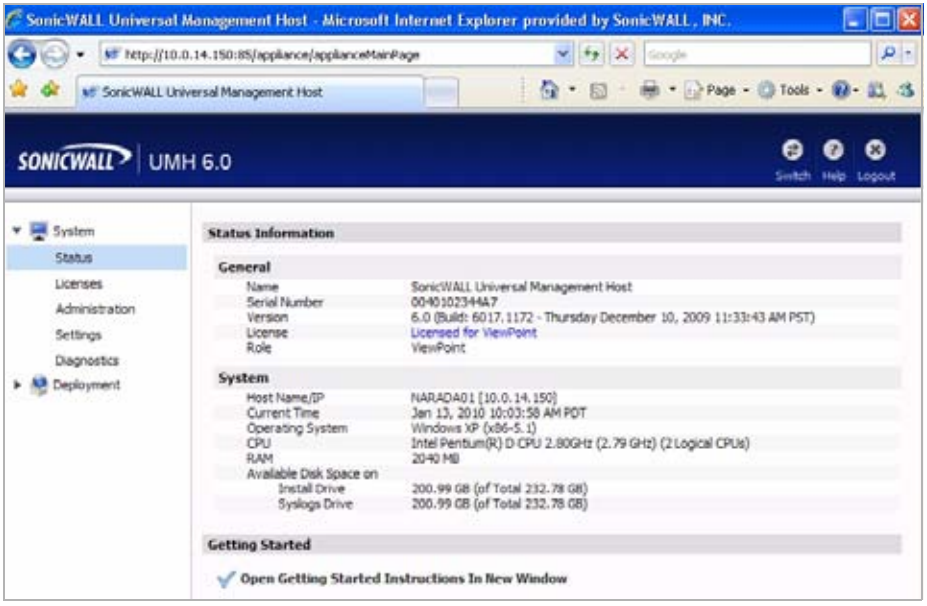
This section describes the tasks you can perform on the System pages of the SonicWALL ViewPoint UMH system interface.

See the following sections:

- Viewing System Status, page 26
- Managing System Licenses, page 26
- Configuring System Administration Settings, page 28
- Managing System Settings, page 29
- Using System Diagnostics, page 30

Viewing System Status

The System > Status page provides the general information about the installation, including the name which identifies the system as a SonicWALL Universal Management Host, the serial number of the SonicWALL ViewPoint instance, the software version, licensing status, and the system role. For SonicWALL ViewPoint, the role is always "ViewPoint."


SonicWALL Universal Management Host - Microsoft Internet Explorer provided by SonicWALL, INC.
http://10.0.14.150:85/appliance/applianceMainPage
SonicWALL Universal Management Host
SONICWALL UMH 6.0
Switch Help Logout
System
Status
Licenses
Administration
Settings
Diagnostics
Deployment
Status Information
General
Name SonicWALL Universal Management Host
Serial Number 0040102344A7
Version 6.0 (Build: 6017.1172 - Thursday December 10, 2009 11:33:43 AM PST)
License Licensed for ViewPoint
Role ViewPoint
System
Host Name/IP NARADA01 (10.0.14.150)
Current Time Jan 13, 2010 10:03:58 AM PDT
Operating System Windows XP (x86-5.1)
CPU Intel Pentium(R) D CPU 2.80GHz (2.79 GHz) (2 Logical CPUs)
RAM 2040 MB
Available Disk Space on
Install Drive 200.99 GB (of Total 232.78 GB)
Syslogs Drive 200.99 GB (of Total 232.78 GB)
Getting Started
Open Getting Started Instructions In New Window

Under System, the host name of the computer is listed, along with the time and other information about the host computer.

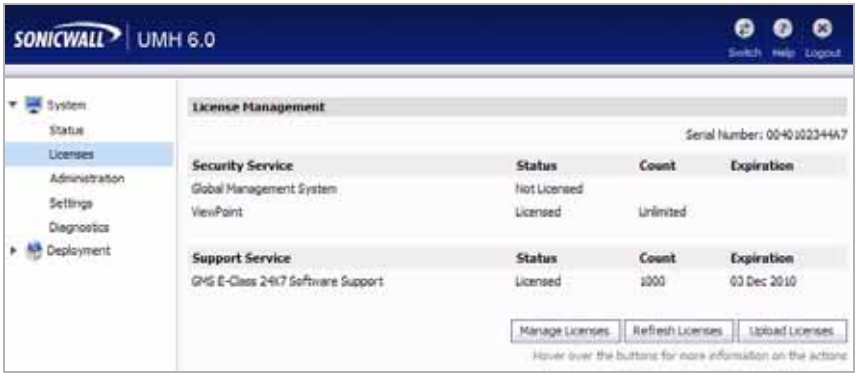
At the bottom of the page, a link is provided to access the *Getting Started Guide* which takes you to the online help table of contents.

Managing System Licenses

The System > Licenses page provides buttons for managing, refreshing, and uploading licenses. The page displays the status of ViewPoint and Global Management System licenses. The Global Management System license status will show the status of your SonicWALL GMS Free Trial, if activated. If you choose to upgrade to SonicWALL GMS, this page will show Global Management System as fully licensed.

The value in the Count column indicates the number of appliances for which this SonicWALL ViewPoint or SonicWALL GMS instance is licensed for reporting or management. For SonicWALL ViewPoint, this value is usually “unlimited”, but for SonicWALL GMS, the base license is either for 10 nodes or 25 nodes, and additional node licenses can be purchased in various increments.

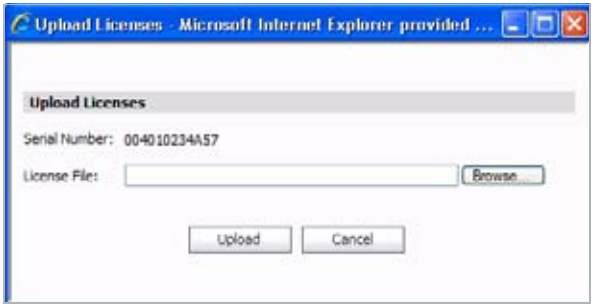
The Expiration column indicates the expiration date of the license. If no date is shown, the license is perpetual, and does not expire.



To display the MySonicWALL login page, click the **Manage Licenses** button. You can purchase licenses and obtain license keysets on MySonicWALL.

Click the **Refresh Licenses** button to refresh the license status on this page.

To upload a new license, click the **Upload Licenses** button and browse to a license file on your computer.



Configuring System Administration Settings

The System > Administration page allows you to configure the system behavior for admin login sessions.

Under Host Settings, enter the number of minutes of inactivity allowed before the session is logged out. A setting of **-1** allows an unlimited amount of inactivity without being logged out.

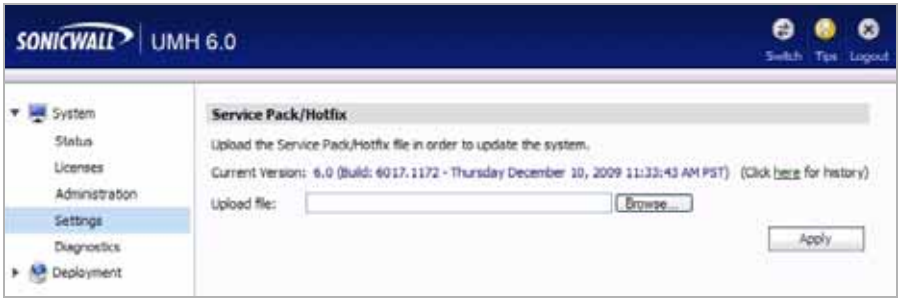
Under Enhanced Security Access, you can configure the number of failed login attempts before the admin account is locked out, and the number of minutes that the lockout lasts. You can also configure the number of days before the admin account password must be changed.

Under Administrator Password, you can change the administrator password for the SonicWALL ViewPoint application. Enter the current password for the system administrator (or root) account into the Current Password field, and then enter the new password into both the **New Password** and **Confirm Password** fields.

After making any changes on this page, click **Update**. To revert the fields on the page to their default settings, click **Reset**.

Managing System Settings

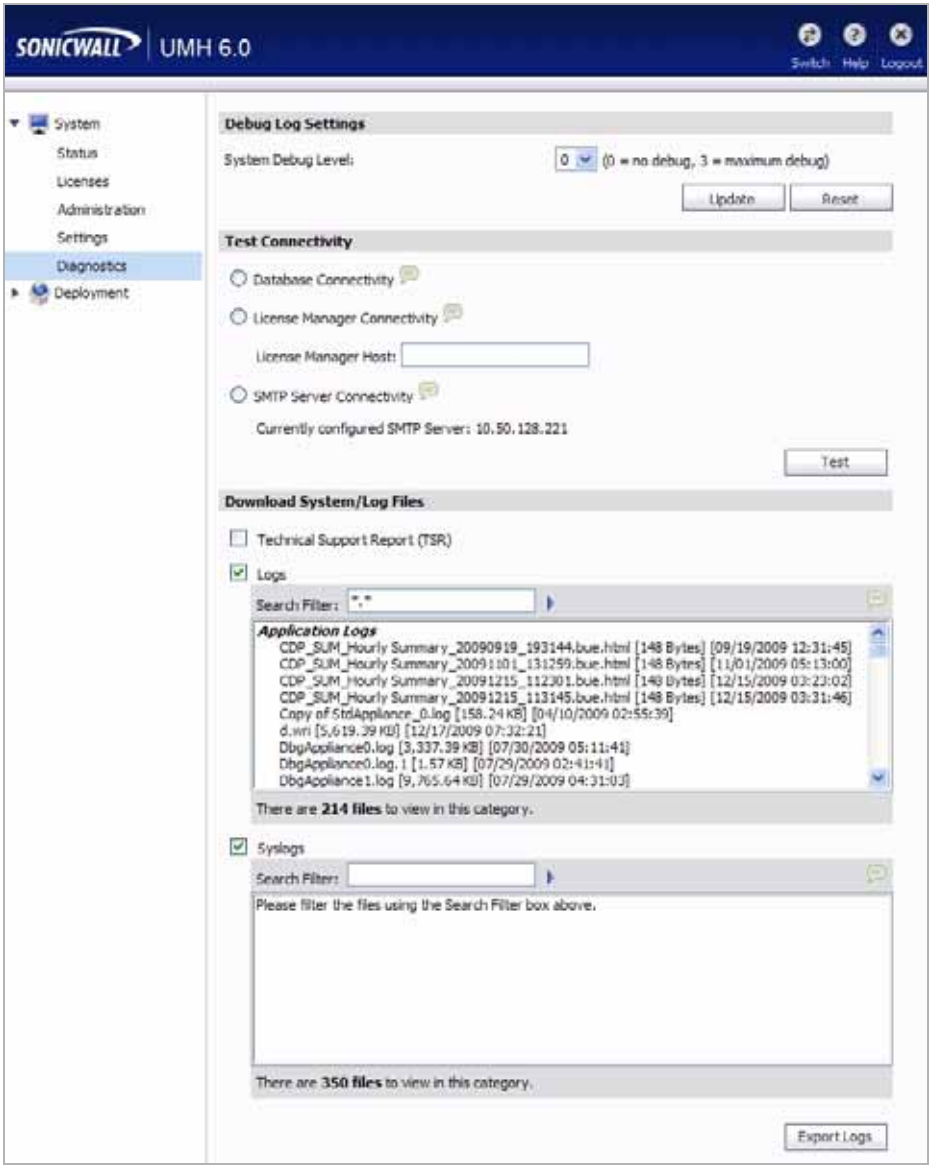
The System > Settings page provides a way to upload new SonicWALL ViewPoint software or service packs to the system. Click **Browse** to browse to the file you wish to upload, and then click **Apply**.



The page shows the current version of SonicWALL UMS, and provides a History link that displays the history of all hotfixes and firmware updates that were applied to the system.

Using System Diagnostics

The System > Diagnostics page is used to set log levels, test connectivity to servers, generate Tech Support Reports, and to search and download system log files.



Under Debug Log Settings, select the log level from the **System Debug Level** drop-down list. You can select **0** for no debug information, **1** or **2** for more, and **3** for maximum debug information.

In the Test Connectivity section, select one of the following radio buttons and then click **Test** to verify connectivity to that server:

- **Database Connectivity** – Tests connectivity to the database server configured on the Deployment > Roles page.
- **License Manager Connectivity** – Type the host name or IP address into the License Manager Host field and click Test to test connectivity to that server.
- **SMTP Server Connectivity** – Tests connectivity to the SMTP server configured on the Deployment > Settings page.

In the Download System/Log Files section, you can enter a filter, or search value, into either of the **Search Filter** fields, and then press **Enter**, to locate log entries of interest. Click the **Export Logs** button to save the log files to a file on your computer.

To generate a TSR (Technical Support Report), select the **Technical Support Report (TSR)** checkbox, and then click **Export Logs**.

Configuring UMH Deployment Options

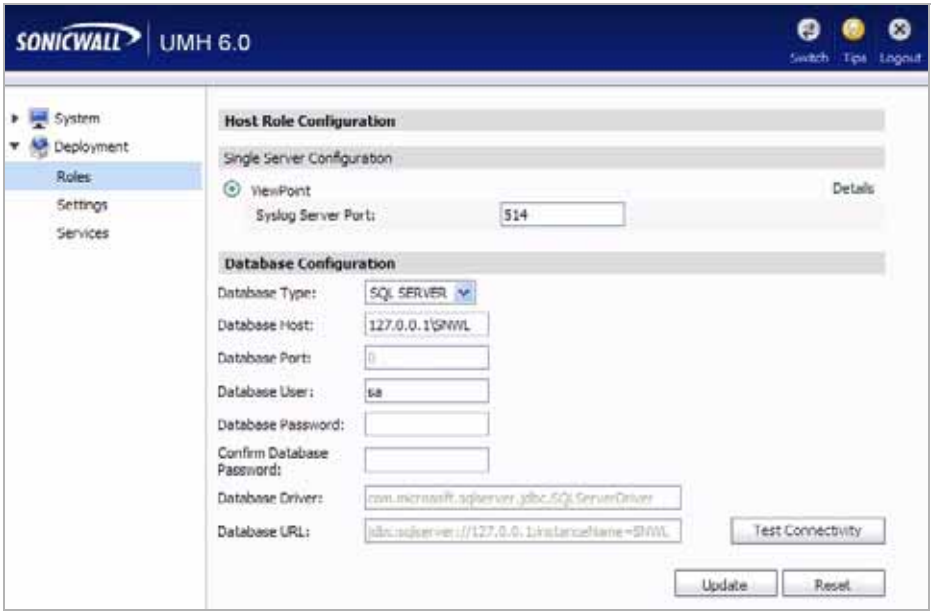
This section describes the tasks you can perform on the Deployment pages of the SonicWALL ViewPoint UMH system interface.

See the following sections:

- Configuring the Deployment Role, page 32
- Configuring Deployment Settings, page 34
- Controlling Deployment Services, page 36

Configuring the Deployment Role

In a SonicWALL ViewPoint installation, the Deployment > Roles page provides a way to configure the syslog port and the database settings, and to test database cnnectivity.



To set the syslog port, enter the port number into the **Syslog Server Port** field.

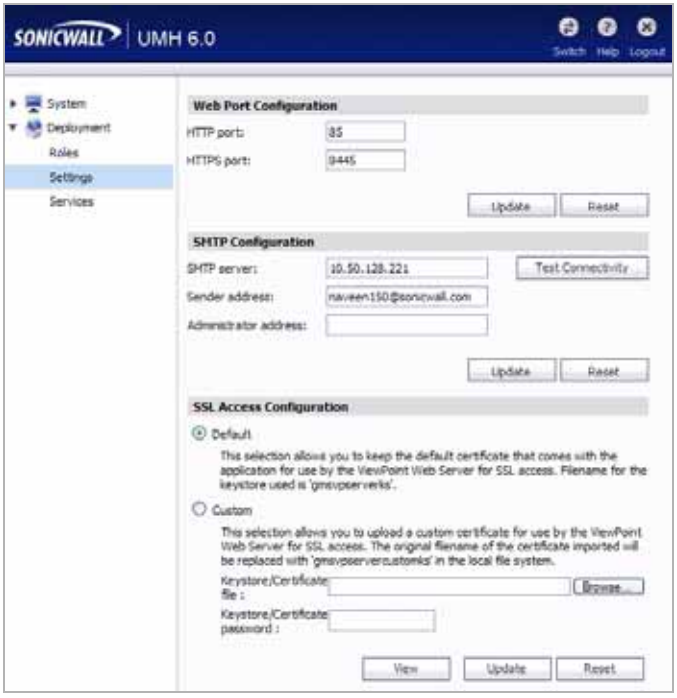
Under Database Configuration, to provide credentials with which SonicWALL ViewPoint will access the database, enter the account user name into the **Database User** field, and enter the account password into both the **Database Password** and **Confirm Database Password** fields.

To test connectivity to the database server, click **Test Connectivity**. A popup will display the status.

When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Configuring Deployment Settings

The Deployment > Settings page provides a way to set the Web ports, the SMTP server IP address with the sender and administrator email addresses, and the SSL access configuration.



To configure the Web ports, enter the desired port numbers into the **HTTP Port** and **HTTPS Port** fields, and then click **Update**.

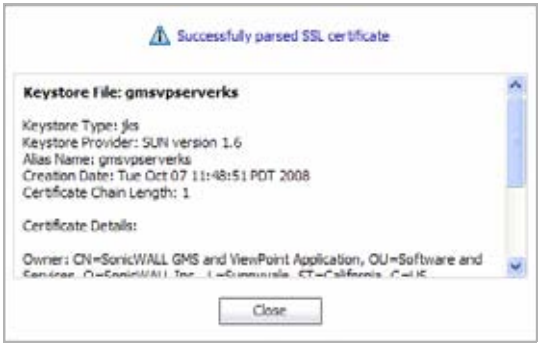
To configure the SMTP settings, perform the following steps:

1. In the **SMTP Server** field, enter the IP address or fully qualified domain name of the SMTP server. This is normally the same server that handles your regular email service.
2. In the **Sender Address** field, enter the email address, including domain, by which SonicWALL ViewPoint will be known when sending email.
3. In the **Administrator Address** field, enter the email address of the administrator who will receive email alerts and other email communications from SonicWALL ViewPoint.
4. Under SSL Access Configuration, select one of the following settings:

- **Default** – Keep the default certificate that comes with the application for use by the ViewPoint Web Server for SSL access. The filename for the keystore is **gmsvpserverks**.
- **Custom** – Upload a custom certificate for use by the ViewPoint Web Server for SSL access. The original filename of the imported certificate is replaced with **gmsvpservercustomks** in the local file system.

  Click **Browse** and select the certificate file for the **Keystore / Certificate file** field and type the password into the **Keystore / Certificate password** field.

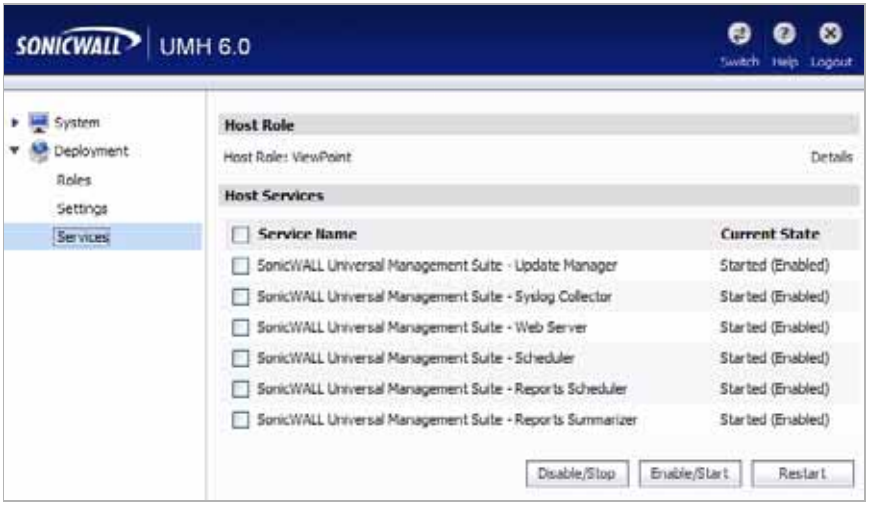
  To display information contained in the certificate, click **View**.


Successfully parsed SSL certificate
Keystore File: gmsvpserverks
Keystore Type: jks
Keystore Provider: SUN version 1.6
Alias Name: gmsvpserverks
Creation Date: Tue Oct 07 11:48:51 PDT 2008
Certificate Chain Length: 1
Certificate Details:
Owner: CN=SonicWALL GMS and ViewPoint Application, OU=Software and
Close

5. When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Controlling Deployment Services

The Deployment > Services page provides a list of the services that are running on your system as part of SonicWALL ViewPoint. It also provides a way to stop or start any of the services.



To stop a service that is currently Enabled, select the checkbox for that service and then click **Disable / Stop**.

To start a service that is currently Disabled, select the checkbox for that service and then click **Enable / Start**.

To restart a service that is either Enabled or Disabled, select the checkbox for that service and then click **Restart**.

CHAPTER 3
Adding SonicWALL Appliances

This chapter describes how to add SonicWALL appliances to SonicWALL ViewPoint. . This chapter contains the following sections:

- "Adding SonicWALL Appliances to SonicWALL ViewPoint" on page 37
- "Deleting SonicWALL Appliances from ViewPoint" on page 39

Adding SonicWALL Appliances to SonicWALL ViewPoint

SonicWALL ViewPoint checks with the SonicWALL licensing server when you add an appliance, so it is important that ViewPoint has Internet access to the server.

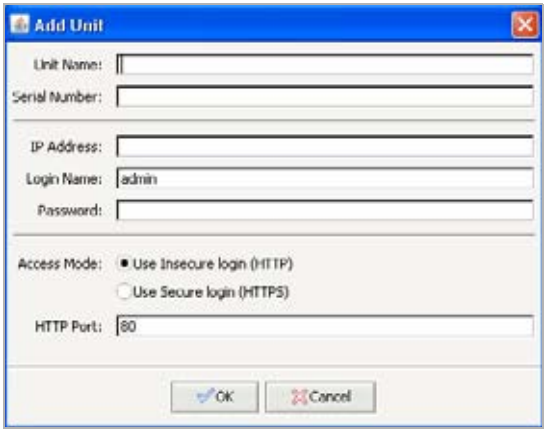
SonicWALL ViewPoint can communicate with SonicWALL appliances through HTTP or HTTPS. See the following sections:

- "Adding SonicWALL Appliances" on page 38
- "Modifying SonicWALL Appliance Settings" on page 39

Adding SonicWALL Appliances

To add a SonicWALL appliance using the SonicWALL ViewPoint management interface, follow these steps:

1. Click the appliance tab that corresponds to the type of appliance that you want to add: **UTM** or **SSL-VPN**.
2. Right-click in the left pane (TreeControl pane) of the SonicWALL ViewPoint management interface and select **Add Unit**. The Add Unit dialog box appears.



3. Enter a descriptive name for the SonicWALL appliance in the **Unit Name** field.

Note Do not enter the single quote character (‘) in the **Unit Name** field.

4. Enter the serial number of the SonicWALL appliance in the **Serial Number** field.
5. Enter the IP address of the SonicWALL appliance in the **IP Address** field.
6. Enter the administrator login name for the SonicWALL appliance in the **Login Name** field.
7. Enter the password used to access the SonicWALL appliance in the **Password** field.
8. For **Access Mode**, select from the following:
   - If the SonicWALL appliance will be connected over HTTP, select **Use Insecure login (HTTP)**.

– If the SonicWALL appliance will be connected over HTTPS, select **Use Secure login (HTTPS)**.

9. Enter the port used to connect to the SonicWALL appliance in the **HTTP(S) Port** field (default ports are HTTP: 80; HTTPS: 443).
10. Click **OK**. The new SonicWALL appliance appears in the SonicWALL ViewPoint management interface. It will have a yellow icon that indicates it has not yet been successfully acquired.

    SonicWALL ViewPoint will then attempt to set up an HTTP or HTTPS connection to access the appliance. ViewPoint then reads the appliance configuration and acquires the SonicWALL appliance for reporting. This will take a few minutes.

    After the SonicWALL appliance is successfully acquired, its icon turns blue, its configuration settings are displayed at the unit level, and its settings are saved to the database.

Modifying SonicWALL Appliance Settings

If you make a mistake or need to change the settings of an added SonicWALL appliance, you can manually modify its settings or how it is managed.

To modify a SonicWALL appliance, perform the following steps:

1. Right-click the appliance name in the left pane of the SonicWALL ViewPoint UI and select **Modify Unit** from the pop-up menu. The Modify Unit dialog box appears.
2. The Modify Unit dialog box contains the same options as the Add Unit dialog box. For descriptions of the fields, see Adding SonicWALL Appliances to SonicWALL ViewPoint, page 37.
3. When you have finished modifying options, click **OK**. The SonicWALL appliance settings are modified.

Deleting SonicWALL Appliances from ViewPoint

To delete a SonicWALL appliance from ViewPoint, perform the following steps:

1. Right-click on a SonicWALL appliance in the left pane and select **Delete** from the pop-up menu.

2. In the warning message that displays, click **Yes**. The SonicWALL appliance is deleted from ViewPoint.

CHAPTER 4

Using the SonicToday Panel

This chapter introduces the SonicToday panel in the SonicWALL ViewPoint management interface. .

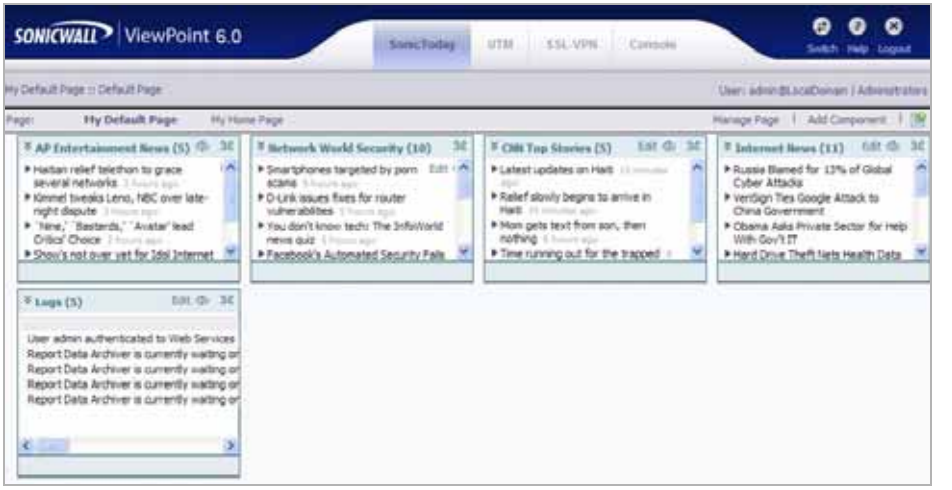
This section includes the following subsections:

- "Overview of the SonicToday Panel" section on page 42
- "Editing a Component Window" section on page 42
- "Adding a Component Window" section on page 44
- "Adding More Pages" section on page 47
- "Editing and Deleting Pages" section on page 48
- "Other Features" section on page 49

Overview of the SonicToday Panel

Using RSS and AJAX technology, SonicToday is a tab intended to work as a customizable dashboard where you are able to monitor the latest happenings with your SonicWALL ViewPoint 6.0 deployment, your network, the IT and Security World, as well as the rest of the world.

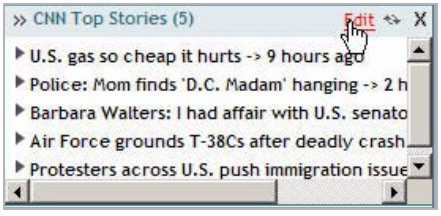
Upon initial login, you see a default **SonicToday** tab. You are able to further customize this page by configuring and adding preferred components.



Editing a Component Window

One customizable feature of SonicToday is the ability to edit the title of any given component window. To do this:

1. Click the **Edit** link, located on the right side of the component window you wish to modify. In this example, we will modify the title of the component window “CNN Top Stories.”

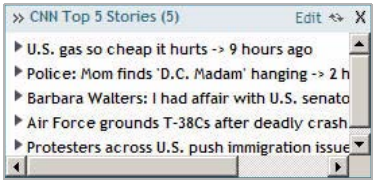

CNN Top Stories (5)
Edit
U.S. gas so cheap it hurts -> 9 hours ago
Police: Mom finds 'D.C. Madam' hanging -> 2 h
Barbara Walters: I had affair with U.S. senato
Air Force grounds T-38Cs after deadly crash
Protesters across U.S. push immigration issue

2. The component window will expand, revealing the following entries you can modify:

Title – The title of the component window.
RSS URL – The URL of the RSS Feed the current component window updates from.
Items – The number of items to be displayed on the component window.
Refresh Interval – The frequency of time the component window will refresh the RSS Feed.

In this example, we will change the title to “CNN Top 5 Stories.” For **Items**, we specify that we want five items shown in the component window, and we want the **Refresh Interval** to occur every 30 minutes. Click **Save** to save your changes and exit the component window.

The changes will update the component window immediately.


» CNN Top 5 Stories (5)
Edit
U.S. gas so cheap it hurts -> 9 hours ago
Police: Mom finds 'D.C. Madam' hanging -> 2 h
Barbara Walters: I had affair with U.S. senato
Air Force grounds T-38Cs after deadly crash
Protesters across U.S. push immigration issue

Adding a Component Window

Another way to fully customize your SonicToday dashboard is by adding a component window specifically to your preferences.

Note that no component containing the same content can be added more than once in the SonicToday dashboard.

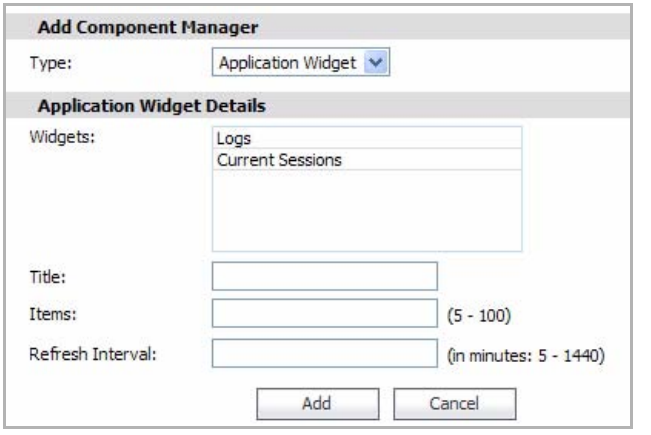
In this section, there are different component windows you can add:

- “Application Widget” section on page 44
- “RSS Feed” section on page 46

Application Widget

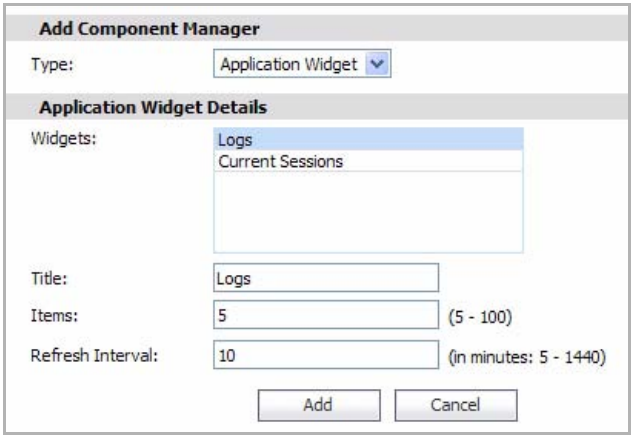
The application widget specifically details Logs and Current Sessions in SonicWALL ViewPoint 6.0. The convenience of this new widget is that it enables you to keep track of all these different details from the SonicToday dashboard page, rather than navigating through other tabs. To add the application widget:

1. Click **Add Component** to bring up the Add Component Manager dialogue box. Select **Application Widget** from the ‘Type’ drop-down list.

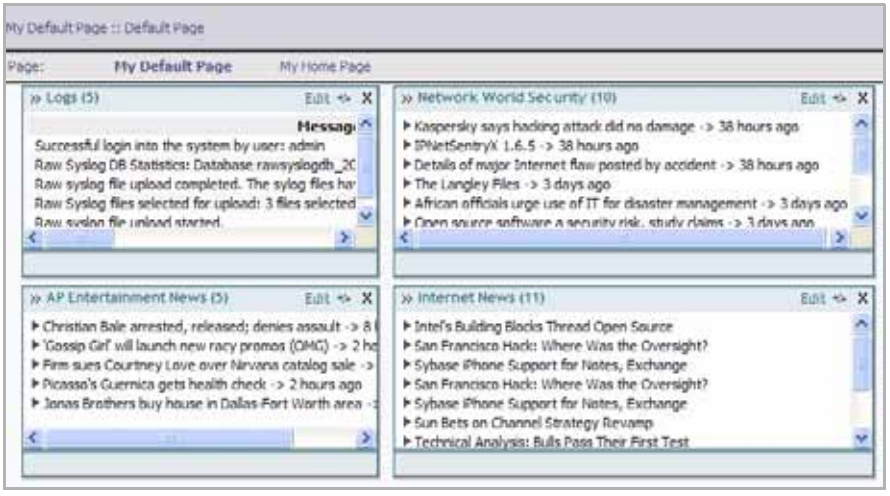


2. Specify what type of **Widget** you want in the component. The **Title** will default to the Widget you choose, but you may customize this if you prefer. You also will indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval**.

   In this example, we will add a widget that monitors Logs, displaying the latest five everyten minutes.



3. Click **Add** when finished specifying entries. The component window is added to the SonicToday dashboard.



RSS Feed

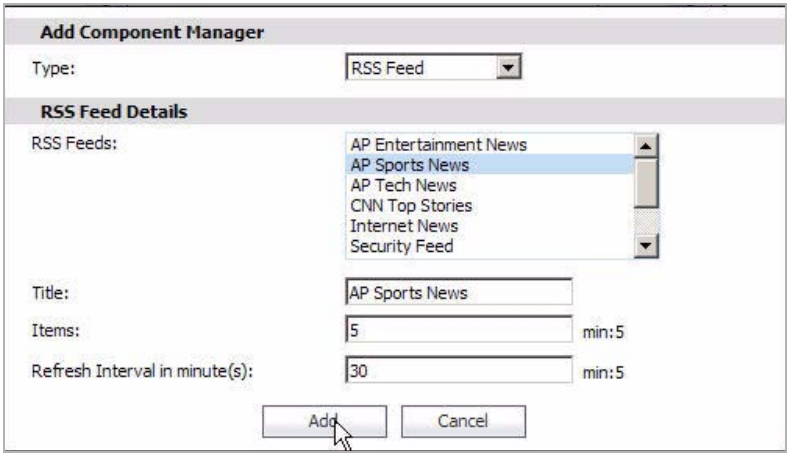
RSS Feed is a component window designed to keep you updated with what is going on in the IT and Security World, as well as all around the globe. This section contains procedures for customizing an RSS Feed component window on your SonicToday dashboard.

To choose a Predefined RSS Feed:

1. Click **Add Component** to bring up the Add Component Manager dialogue box.
2. Select **RSS Feed** from the 'Type' drop-down list. This will automatically bring up a list of predefined RSS Feeds you may choose from.

   The **Title** will default to the Alert Type you choose, but you may customize this if you prefer. You also will indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval**.

   In this example, we will select 'AP Sports News,' displaying the first five items every 30 minutes on the component window.



3. Click **Add** when you are finished. This will add the new RSS Feed component window to your SonicToday dashboard.

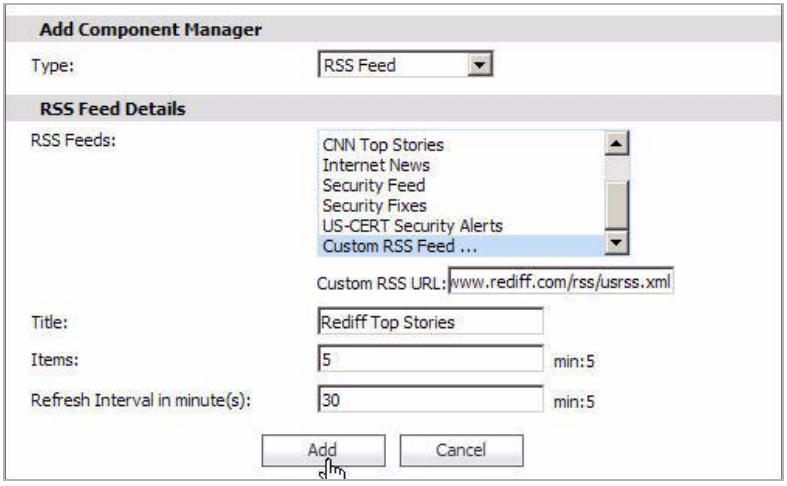
To Choose a Custom RSS Feed:

1. Click **Add Component** to bring up the Add Component Manager dialogue box.
2. Select **RSS Feed** from the 'Type' drop-down list. This will automatically bring up a list of predefined RSS Feeds you may choose from.
3. Scroll to the bottom of the predefined list and select **Custom RSS Feed...** Enter the URL of the RSS Feed you would like on your component window.

Note To search a large directory of available RSS Feeds, navigate to: http://www.rsfeeds.com/

4. Enter the **Title** for this custom RSS Feed page. Also indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval**.

   In this example, we will choose 'Rediff Top Stories,' displaying the first five items every 30 minutes on the component window.



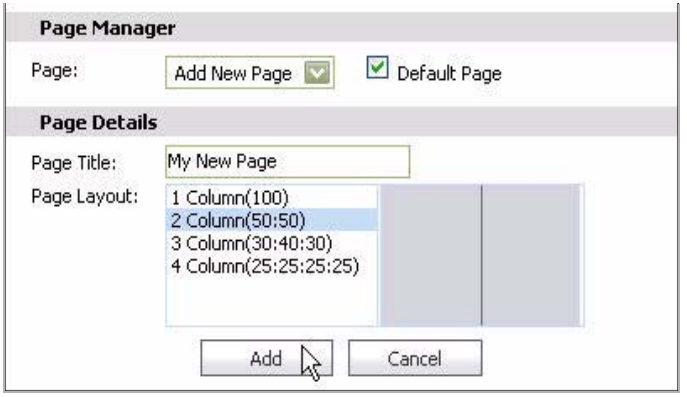
5. Click **Add** when you are finished. This will add the new RSS Feed component window to your SonicToday dashboard.

Adding More Pages

SonicToday allows you to create more pages in addition to your default dashboard page. Note that only one page may be designated as your SonicToday default page. As soon as a new page is marked as the default, any previous default page settings are overwritten. To create a new page:

1. Click **Manage Page** from the toolbar to bring up the Page Manager.
2. In the 'Page' section, select **Add New Page** from the drop-down list.
3. Name your new page under 'Page Title.'
4. Select the layout of your page under 'Page Layout.' A thumbnail image pops up alongside each option to assist you.

5. You also have the option of making this your default page, simply by placing a checkmark in the box labeled ‘Default Page.’



6. Click **Add** when you are finished. The toolbar now displays the newly added page.
In this example, we titled the new page ‘News.’

You can now add and customize component windows to navigate between pages.

Editing and Deleting Pages

To edit a page, click **Manage Page** from the toolbar. Select the page you wish to edit, make your changes, and click **Edit** to finish.

To delete a page, click **Manage Page** from the toolbar. Select the page you wish to delete and click **Delete**. Click **OK** to finish.

Other Features

See the following sections:

- AutoHide, page 49
- Page Selector, page 49
- Component Height Resize, page 50
- Manual Refresh, page 50
- Removing or Deleting a Component, page 50
- Minimizing or Maximizing a Component, page 50

AutoHide

AutoHide is a feature you customize by turning on or off. When AutoHide is turned on, the control bar will hide after an interval of two seconds when the mouse is moved away from the control bar. When AutoHide is turned off, the control bar always appears on the SonicToday dashboard.

To turn AutoHide on, click the **Off** icon .

To turn AutoHide off, click the **On** icon

Page Selector

Whenever the number of pages added to the SonicToday dashboard exceeds five, a page selector bar appears at the top of the main window with left and right arrows. The arrows can be used to scroll across different pages in both directions. By default, the selector is scrolled to a point where the default page appears on it. Any page can be selected by clicking on the page title.

Component Height Resize

The height of a component can be increased and decreased by stretching or shrinking the resize cursor on the status bar when the mouse is moved over the status bar.

Internet News (10)
Edit
Yahoo, Icahn Declare Cease-fire in Proxy War
SAP Shutters Division Amid Oracle Lawsuit
Facebook Revamp Targets Spam, Privacy Issues
Apple Investors to Look for Clues on Jobs' Health
Yahoo, Icahn Settle; Microsoft Out?
Is Open Source Development Insecure?
Are Enterprises Effectively Tapping the Social?
Is Open Source Development Insecure?
NTT Donates IPv6 Bandwidth to Open Source
Tech Stocks Follow Microsoft, Google Lower

Manual Refresh

Aside from the automatic refresh, which you configure in the "Editing a Component Window" section on page 42, you can force a refresh on the component window by clicking the **refresh** icon on the component window header.

Removing or Deleting a Component

Any component window can be removed or deleted from the page by clicking the **close** icon on the component window header.

Minimizing or Maximizing a Component

Each component can be in minimized or maximized state. The components are loaded in the page with the state they were saved in the database.

To minimize a component window, click the **minimize** icon in the component window header.

To maximize a component window, click the **maximize** icon in the component window header.

CHAPTER 5
Configuring User Settings

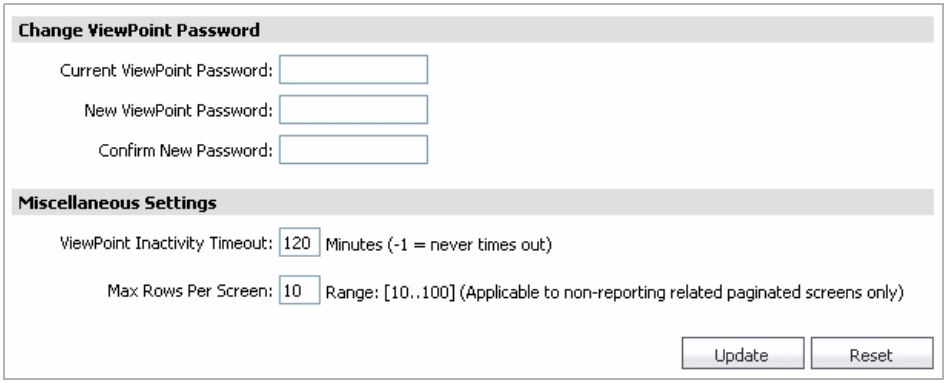
This chapter describes how to configure the user settings that are available in the Console panel on the User Settings screens.

This chapter includes the following sections:

- "Configuring General Settings" section on page 51
- "Configuring Reports Settings" section on page 53

Configuring General Settings

This section describes the **User Settings > General** page, which provides a way to change the ViewPoint administrator password, the ViewPoint inactivity Timeout, and pagination settings.



Perform the following steps:

1. Enter the existing SonicWALL ViewPoint password in the **Current ViewPoint Password** field.
2. Enter the new SonicWALL ViewPoint password in the **New ViewPoint Password** field.
3. Reenter the new password in the **Confirm New Password** field.

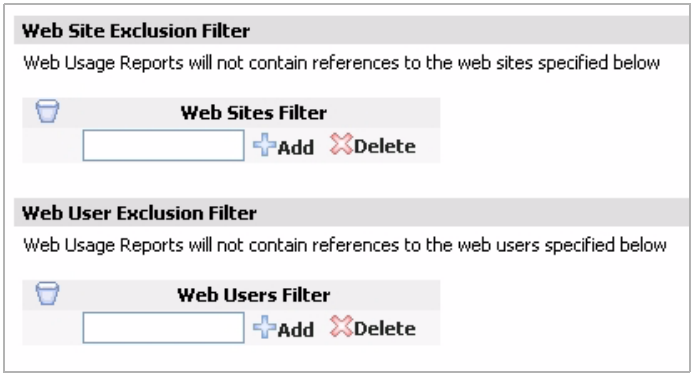
Note Password fields will be grayed out for users on a Remote Domain.

4. The ViewPoint Inactivity Timeout period specifies how long SonicWALL ViewPoint waits before logging out an inactive user. To prevent someone from accessing the SonicWALL ViewPoint UI when SonicWALL ViewPoint users are away from their desks, enter an appropriate value in the **ViewPoint Inactivity Timeout** field. You can disable automatic logout completely by entering a “-1” in this field. The minimum is 5 minutes and the maximum is 120 minutes.
5. Select a value between 10 and 100 in the **Max Rows Per Screen** field. This value applies only to non-reporting related paginated screens.
6. When you are finished, click **Update**. The settings are changed. To clear all screen settings and start over, click **Reset**.

Note The maximum size of the SonicWALL ViewPoint User ID is 24 alphanumeric characters. The password is one-way hashed and any password of any length can be hashed into a fixed 32 character long internal password.

Configuring Reports Settings

The User Settings > Reports page on the Console panel provides settings for the Web Site Exclusion Filter and Web User Exclusion Filter. Web Usage reports will not contain references to the Web sites or users specified on this page.


Web Site Exclusion Filter
Web Usage Reports will not contain references to the web sites specified below
Web Sites Filter
Add
Delete
Web User Exclusion Filter
Web Usage Reports will not contain references to the web users specified below
Web Users Filter
Add
Delete

The following Web Usage reports are affected by the Web Site and Web User Exclusion Filters:

- Web Usage > Summary
- Web Usage > Top Sites
- Web Usage > Top Users
- Web Usage > By User
- Web Usage > By Site
- Web Usage > By Category
- Web Usage > Over Time
- Web Usage > Top Sites Over Time
- Web Usage > Top Users Over Time
- Web Usage > By User Over Time
- Web Usage > By Category Over Time

Adding Web Sites to the Filter List

When entering the Web site to exclude, type only the site name. The filter will search for the exact value provided. In the reports, only the site name is listed, without the http:// or www prefix. So for example, http://site1.sonicwall.com would not find a match in any reports because it would be listed in the reports simply as site1.sonicwall.com.

To add a Web site to the Web Sites Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, type the Web site to be excluded into the **Web Sites Filter** field.

   Enter the Web site without the http:// or www prefix.

2. Click the **Add** button.

Deleting Web Sites from the Filter List

To remove a Web site from the Web Sites Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, select the checkbox next to the Web site to be removed from the exclusion list. To select all sites in the list, select the **Select All** checkbox.
2. Click the **Delete** button.

Adding Web Users to the Filter List

To add a user to the Web Users Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, type the user name to be excluded into the **Web Users Filter** field.

   Enter the user name without the domain.

2. Click the **Add** button.

Deleting Web Users from the Filter List

To remove a Web user from the Web Users Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, select the checkbox next to the user to be removed from the exclusion list. To select all users in the list, select the **Select All** checkbox.
2. Click the **Delete** button.

CHAPTER 6
Configuring Log Settings

This section describes how to configure Log Settings. This includes adjusting settings on deleting log messages after a certain period of time, and setting criteria for viewing logs.

This chapter includes the following sections:

- "Configuration" section on page 57
- "View Log" section on page 58

Configuration

The Log > Configuration screen provides a way to delete log messages older than a specific date.

To delete ViewPoint log messages, perform the following steps:

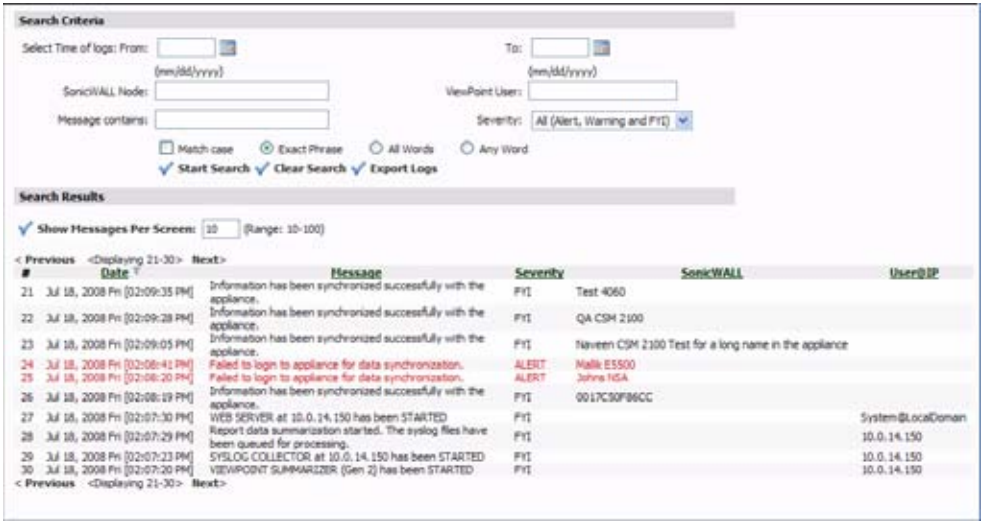
1. Click the **Console** tab, expand the **Log** tree, and click **Configuration**. The Configuration page displays.

2. Select the month, day, and year from the drop down menu.
3. Click **Delete Log Messages Older Than**.

View Log

The SonicWALL ViewPoint log keeps track of changes made within the SonicWALL ViewPoint UI, logins, failed logins, logouts, password changes, scheduled tasks, failed tasks, completed tasks, raw syslog database size, syslog message uploads, and time spent summarizing syslog data. To view the SonicWALL ViewPoint log, perform the following steps:

1. Click the Console tab, expand the Log tree, and click **View Log**. The View Log page displays.


Search Criteria
Select Time of logs: From:
To:
(mm/dd/yyyy)
SonicWALL Node:
ViewPoint User:
Message contains:
Severity:
All (Alert, Warning and FYI)
Match case
Exact Phrase
All Words
Any Word
Start Search
Clear Search
Export Logs
Search Results
Show Messages Per Screen:
(Range: 10-100)
< Previous
<Displaying 21-30>
Next>
Date Message Severity SonicWALL User@IP
21 Jul 18, 2008 Fri [02:09:35 PM] Information has been synchronized successfully with the appliance. FYI Test 4060
22 Jul 18, 2008 Fri [02:09:28 PM] Information has been synchronized successfully with the appliance. FYI QA CSM 2100
23 Jul 18, 2008 Fri [02:09:05 PM] Information has been synchronized successfully with the appliance. FYI Naveen CSM 2100 Test for a long name in the appliance
24 Jul 18, 2008 Fri [02:08:41 PM] Failed to login to appliance for data synchronization. ALERT Malik E5500
25 Jul 18, 2008 Fri [02:08:20 PM] Failed to login to appliance for data synchronization. ALERT Johns NSA
26 Jul 18, 2008 Fri [02:08:19 PM] Information has been synchronized successfully with the appliance. FYI 0017C50F86CC
27 Jul 18, 2008 Fri [02:07:30 PM] WEB SERVER at 10.0.14.150 has been STARTED FYI System@LocalDomain
28 Jul 18, 2008 Fri [02:07:29 PM] Report data summarization started. The syslog files have been queued for processing. FYI 10.0.14.150
29 Jul 18, 2008 Fri [02:07:23 PM] SYSLOG COLLECTOR at 10.0.14.150 has been STARTED FYI 10.0.14.150
30 Jul 18, 2008 Fri [02:07:20 PM] VIEWPOINT SUMMARIZER (Gen 2) has been STARTED FYI 10.0.14.150
< Previous
<Displaying 21-30>
Next>

2. Each log entry contains the following fields:
   - #—specifies the number of the log entry.
   - **Date**—specifies the date of the log entry.
   - **Message**—contains a description of the event.
   - **Severity**—displays the severity of the event (Alert, Warning, or FYI).
   - **SonicWALL**—specifies the name of the SonicWALL appliance that generated the event (if applicable).
   - **User@IP**—specifies the user name and IP address.
3. To narrow the search, configure some of the following criteria:

Tip You can press Enter to navigate from one form element to the next in this section.

- **Select Time of logs**—displays all log entries for a specified range of dates.
- **SonicWALL Node**—displays all log entries associated with the specified SonicWALL appliance.
- **ViewPoint User**—displays all log entries with the specified user.
- **Message contains**—displays all log entries that contain the specified text. This input field provides an auto-suggest functionality that uses existing log message text to predict what you want to type. It fills in the field with the suggested text and you can either press **Tab** to accept it or keep typing. Different suggestions will appear as you continue to type if log messages match your input.
- **Severity**—displays log entries with the matching severity level:
  - All (Alert, Warning, and FYI)–where FYI mean “For Your Information”
  - Alert and Warning
  - Alert
- Select the **Match case** checkbox to make the **SonicWALL Node**, **ViewPoint User**, and **Message contains** search fields case sensitive.
- Select one of **Exact Phrase**, **All Words**, or **Any Word**.
  - **Exact Phrase** matches a log entry that contains exactly what you typed in the **Message contains** field
  - **All Words** matches a log entry that contains all the words you typed in the **Message contains** field, but the words can be non-consecutive or in any order
  - **Any Word** matches a log entry that contains any of the words you typed in the **Message contains** field

4. To view the results of your search criteria, click **Start Search**. To clear all values from the input fields and start over, click **Clear Search**. To save the results as an HTML file on your system, click **Export Logs** and follow the on-screen instructions.
5. To configure how many messages are shown per screen, enter a new value between 10 and 100 in the **Show Messages Per Screen** field. (default: 10). Click **Next** to display the next page, or click **Previous** to display the preceding page.

CHAPTER 7
Configuring Management Settings

This chapter describes the settings available on the Console panel in the Management section. The following sections are found in this chapter:

- "Settings" section on page 61
- "Alert Settings" section on page 64
- "Sessions" section on page 65
- "Database Maintenance" section on page 66

Settings

On the Console > Management >Settings page, you can configure email settings, set the system debug level, synchronize model codes information, and configure password security settings..

This section describes the following Settings topics:

- "Configuring Email Settings" on page 62
- "Configuring System Debug Level" on page 62
- "Enforcing Password Security" on page 63
- "Synchronizing Model Codes" on page 63

Configuring Email Settings

An SMTP server and an email address are required for sending ViewPoint reports.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your SonicWALL ViewPoint deployment performance
- Availability of product updates, hot fixes, or patches
- Scheduled Reports

To configure these email settings:

1. Click the **Console** tab.
2. Expand the **Management** tree and click **Settings**. The Settings page displays.
3. Type the IP address of the Simple Mail Transfer Protocol (SMTP) server into the **SMTP Server** field. This server can be the same one that is normally used for email in your network.
4. Type the email account name and domain that will appear in messages sent from the SonicWALL ViewPoint into the **ViewPoint Sender's e-Mail Address** field.
5. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Configuring System Debug Level

SonicWALL ViewPoint provides the **System Debug level** option to control the debug messages sent to the log file.

To configure this setting:

1. Select a debug level from the **System Debug level** drop-down list. The range is 0-3 where a level of 0 provides no debug log messages and a level of 3 provides the maximum number of debug messages.
2. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Enforcing Password Security

SonicWALL ViewPoint supports enforced password rotation for enhanced security compliance.

To enable and configure enforced password rotation:

1. Select the **Enforce Password Security** checkbox.
2. In the **Number of days to force password change** field, enter a value. The default is 90. SonicWALL ViewPoint will prompt the administrator to change the admin account password after the specified number of days.
3. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Synchronizing Model Codes

The Sync Model Codes feature accommodates new SonicWALL product introductions without the need for ViewPoint update. When SonicWALL updates the the corporate server (MySonicWALL) with a new product code, it then becomes available to ViewPoint. The task is scheduled to run every 24 hours and is also available manually.

To synchronize model codes immediately:

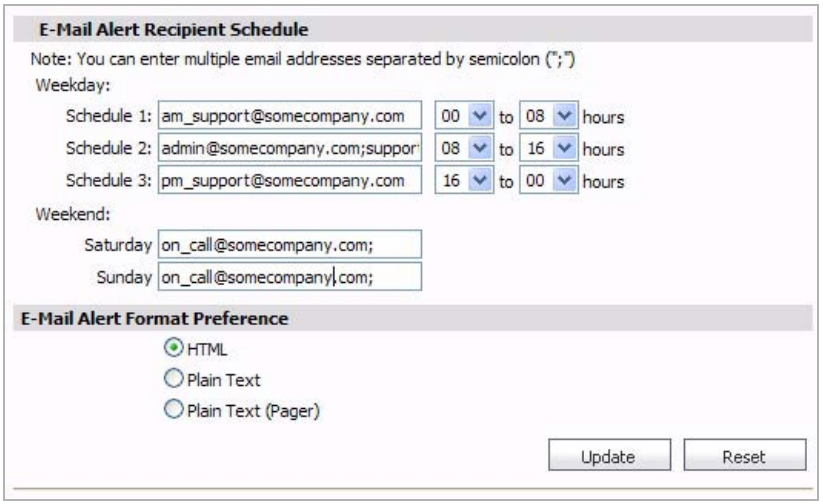
1. On the Console > Management > Settings page, click **Sync Model Codes information now**.
2. A short time later the page is updated to display the synchronization status at the top.

Alert Settings

The Alert Settings page specifies which email addresses receive email alerts and notifications during specific times.

To configure the alert notification settings, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Alert Settings**. The Alert Settings page displays.



2. Configure the email address(es) that will receive notifications and the times that they will receive them:
   - **Schedule 1**—Specifies who will receive notifications during the first weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 2**—Specifies who will receive notifications during the second weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 3**—Specifies who will receive notifications during the third weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Saturday**—Specifies who will receive notifications on Saturday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Sunday**—Specifies who will receive notifications on Sunday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.

3. Select whether the email alert will be sent as **HTML**, **Plain Text**, or **Plain Text (Pager**). The Pager setting sends a very short email to ensure that the email is not cut off by the character limits of some pagers.
4. When you are finished, click **Update**. The settings are saved.

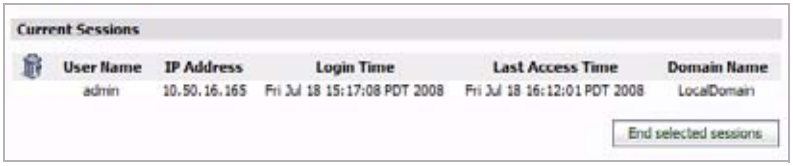
Sessions

The Sessions page of the Management section of the ViewPoint Console allows you to view session statistics for currently logged in ViewPoint users and to end selected sessions.

Managing Sessions

On occasion, it may be necessary to log off other user sessions. To do this, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Sessions**. The Sessions page displays.



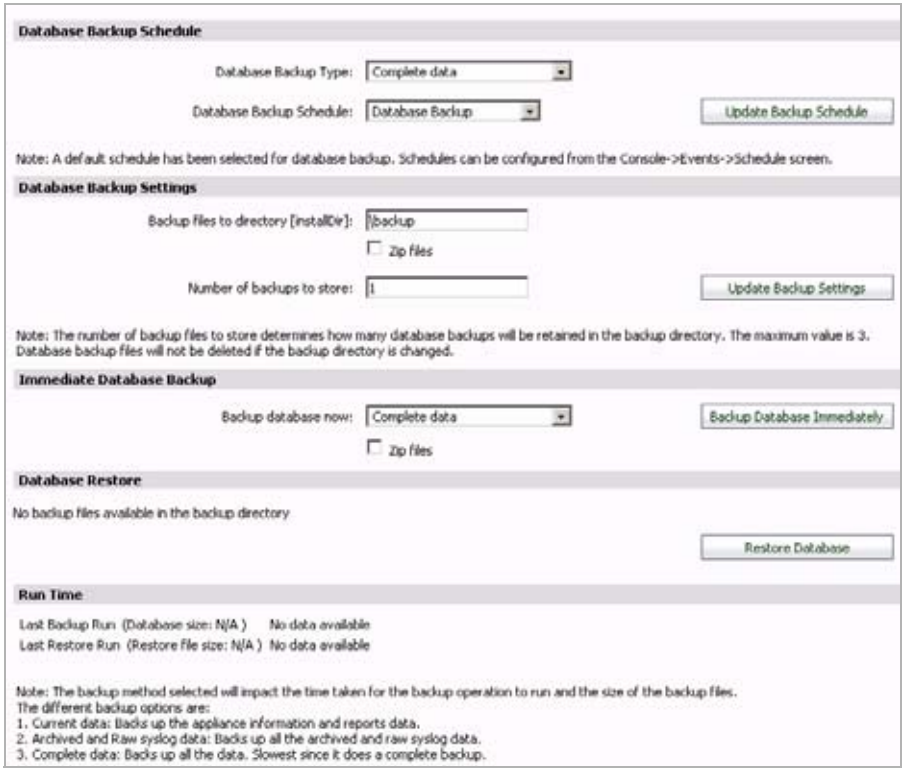
2. When more than one session is active, a checkbox is displayed next to each row. Select the check box of each user to log off and click **End selected sessions**.

   The selected users are logged off.

Database Maintenance

The Database Maintenance page allows you to back up the MySQL databases used by SonicWALL ViewPoint. This screen is not applicable to deployments using SQL Server.

Note The Console > Management > Database Maintenance page only appears in the management interface when a MySQL database is being used.


Database Backup Schedule
Database Backup Type:
Complete data
Database Backup Schedule:
Database Backup
Update Backup Schedule
Note: A default schedule has been selected for database backup. Schedules can be configured from the Console->Events->Schedule screen.
Database Backup Settings
Backup files to directory [installDir]:
\backup
Zip files
Number of backups to store:
1
Update Backup Settings
Note: The number of backup files to store determines how many database backups will be retained in the backup directory. The maximum value is 3. Database backup files will not be deleted if the backup directory is changed.
Immediate Database Backup
Backup database now:
Complete data
Backup Database Immediately
Zip files
Database Restore
No backup files available in the backup directory
Restore Database
Run Time
Last Backup Run (Database size: N/A) No data available
Last Restore Run (Restore file size: N/A) No data available
Note: The backup method selected will impact the time taken for the backup operation to run and the size of the backup files.
The different backup options are:
1. Current data: Backs up the appliance information and reports data.
2. Archived and Raw syslog data: Backs up all the archived and raw syslog data.
3. Complete data: Backs up all the data. Slowest since it does a complete backup.

You can configure the type of backup, schedule for periodic backups, folder for backup storage, and number of backups (up to 3) to keep. You can also perform an immediate database backup from this page. Existing backups of the database are listed, and you can select from them to restore your databases.

See the following sections:

- Configuring Backup Schedule and Settings, page 67
- Backing Up a Database Immediately, page 68
- Restoring a Database Backup, page 68

If you have a SonicWALL UMA appliance, you can download and run the Data Export Wizard. The wizard will help you configure a Java-based client and a corresponding script that you can use to schedule recurring, automatic backups. For information about the Data Export Tool see the "Data Export Wizard" section on page 91.

Configuring Backup Schedule and Settings

To configure the database backup schedule and settings, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree, and click **Database Maintenance**. The Database Maintenance page displays.
2. Under Database Backup Schedule, select one of the following from the **Database Backup Type** drop-down list:
   - **Current data** – Backs up system information and all data in **sgmsdb** for the current month; **sgmsdb** contains summarized report data
   - **Archived and Raw syslog data** – Backs up the archived data that is moved from **sgmsdb** to other files at the end of every month, and backs up raw syslog data
   - **Complete data** – Backs up all data including **sgmsdb** and all archived data and raw syslog data; this option requires the most time
3. Select the desired backup schedule from the **Database Backup Schedule** drop-down list. You can select a pre-configured schedule or a custom schedule, which you can configure in the Console > Events > Schedule screen.
4. When finished selecting options under Database Backup Schedule, click the **Update Backup Schedule** button.
5. Under Database Backup Settings in the **Backup files to directory [installDir]** field, enter the folder name in which you want to store the backup files.
6. Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.

7. In the **Number of backups to store** field, enter the number of backups you want to store. The maximum is 3. When the maximum number of backups is reached in the configured folder, the oldest one will be removed when a new backup is created. If the folder is changed, existing backups in the previous folder will not be deleted.
8. When finished selecting options under Database Backup Settings, Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.
9. When finished selecting options under Database Backup Settings, click the **Update Backup Settings** button.

Backing Up a Database Immediately

To perform an interactive backup of a database, complete the following steps:

1. On the Console > Management > Database Maintenance page, under **Immediate Database Backup**, select the type of backup from the **Backup database now** drop-down list. You can select one of the following types:
   - **Current data** – Backs up system information and all data in **sgmsdb** for the current month; **sgmsdb** contains summarized report data
   - **Archived and Raw syslog data** – Backs up the archived data that is moved from **sgmsdb** to other files at the end of every month, and backs up raw syslog data
   - **Complete data** – Backs up all data including **sgmsdb** and all archived data and raw syslog data; this option requires the most time
2. Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.
3. Click the **Backup Database Immediately** button.
4. In the confirmation dialog box, click **OK**.

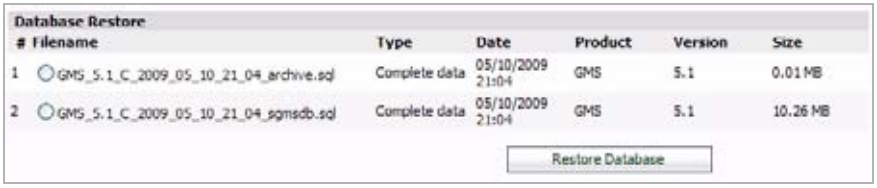
Restoring a Database Backup

This feature allows the administrator to restore a previously backed-up database file.

Note All services except the Web Server and the Database Service should be manually stopped before restoration is started to avoid corruption of data.

To restore your database with one of your backups, perform the following steps:

1. On the **Console > Management > Database Maintenance** page, under **Database Restore**, select the radio button for the backup that you want to restore.



2. Click the **Restore Database** button.
3. In the confirmation dialog box, click **OK**.
4. You must restart the Web Server service manually after the backup is completed.

CHAPTER 8
Managing Reports in the Console Panel

This section describes how to configure reporting settings on the Console panel. These include how often the summary information is updated, the number of days that summary information is stored, and the number of days that raw data is stored.

The following sections are included in this chapter:

- "Settings" section on page 71
- "Summarizer" section on page 73
- "Email/Archive" section on page 81
- "Scheduled Reports" section on page 82
- "Management" section on page 87

Settings

The Settings page under Reports on the Console panel provides a check box for enabling the sort option in report tables. You can also specify the number of appliances which can have Log Viewer enabled at the same time.

See the following:

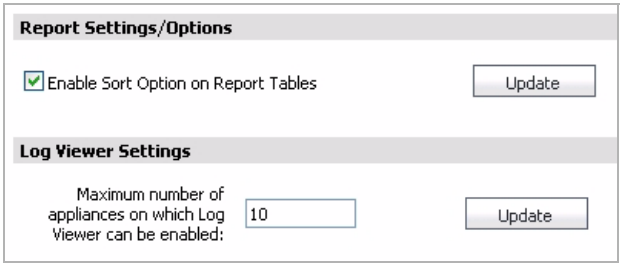
- "Enabling Report Table Sorting" section on page 72
- "Controlling the Number of Appliances with Log Viewer Enabled" section on page 72

Enabling Report Table Sorting

The Report Settings/Options section of the Console > Reports > Settings page provides a checkbox to enable the sort option on report tables.

To enable or disable the sort option for report tables, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Settings**.



2. To enable the report table sort option, select the **Enable Sort Option on Report Tables** checkbox. To disable sorting, clear the checkbox.
3. Click **Update**.

Controlling the Number of Appliances with Log Viewer Enabled

You can control the maximum number of managed appliances for which Log Viewer can be enabled. The default setting allows Log Viewer to be enabled on up to five appliances. Because enabling Log Viewer causes raw syslog data uploading, it is resource intensive. Use care in increasing this number, and when enabling Log Viewer on systems.

Log Viewer must be enabled on an appliance in order to use Custom Reports. Custom Reports are available for UTM and SSL-VPN appliances. For more information about Custom Reports, see the following:

- “Using Custom Reports on UTM Appliances” section on page 163

To change the number of appliances for which Log Viewer can be enabled:

1. On the **Console** panel, navigate to **Reports > Settings**.
2. Under **Log Viewer Settings**, in the **Maximum number of appliances on which Log Viewer can be enabled** field, enter the number of appliances for which Log Viewer can be enabled. The default is five.
3. Click **Update**.

Note Limiting the number of appliances for which the Log Viewer is enabled will increase the overall performance of your SonicWALL ViewPoint system.

Summarizer

This section contains the following subsections:

- "About Summary Data in Reports" on page 73
- "Summarizer Settings and Summarization Interval" on page 73
- "Configuring the Syslog Deletion Schedule Settings" on page 78
- "Configuring Host Name Resolution" on page 79

About Summary Data in Reports

These reports are constructed from the most current available summary data. In order to create summary data, the ViewPoint Reporting Module must parse the raw data files.

When configuring ViewPoint Reporting using the screens on the Console panel under Reports, you can select the amount of summary information to store. These settings affect the database size, be sure there is adequate disk space to accommodate the settings you choose.

Additionally, you can select the number of days that raw syslog data is stored. The raw data is made up of information for every connection. Depending on the amount of traffic, this can quickly consume an enormous amount of space in the database. ViewPoint creates a new 2 GB database for raw syslog data everyday. Be very careful when selecting how much raw information to store. For information on configuring raw data storage, see "Enabling Report Table Sorting" section on page 72.

Summarizer Settings and Summarization Interval

SonicWALL appliances send their syslog packets to SonicWALL ViewPoint via UDP packets. When summarization is enabled, the Summarizer will process those files and store the data in the summary databases at the interval you specify.

See the following sections:

- “Enabling Report Summarization” section on page 74
- “Setting the Reports Data Summarization Interval” section on page 74
- “Using Summarize Now” section on page 76

Enabling Report Summarization

To globally enable the summarization of report data, which is necessary for viewing reports, perform the following:

1. On the **Console** panel, navigate to **Reports > Summarizer**.
2. Under **Summarizer Settings**, select the **Enable Report Summarization** checkbox.
3. Click **Update**.

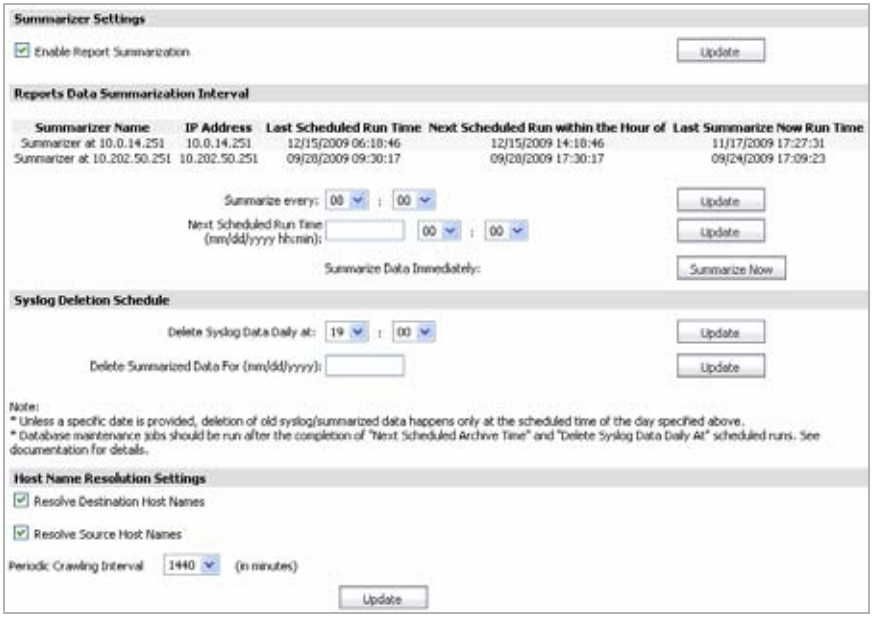
Setting the Reports Data Summarization Interval

The Summarizer will process syslog data sent from SonicWALL appliances and store the processed data in the summary databases at the interval you specify. When an appliance is configured to communicate with ViewPoint, you need to verify that the summarizer is scheduled to collect and process data for this unit at an appropriate interval.

To configure reports for summarization, see the “Selecting Reports for Summarization” section on page 137 in the Scheduling and Configuring Reports chapter.

To configure the summarization interval, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Summarizer**. The Summarizer page displays.


Summarizer Settings
Enable Report Summarization
Update
Reports Data Summarization Interval
Summarizer Name
IP Address
Last Scheduled Run Time
Next Scheduled Run within the Hour of
Last Summarize Now Run Time
Summarizer at 10.0.14.251
10.0.14.251
12/15/2009 06:18:46
12/15/2009 14:18:46
11/17/2009 17:27:31
Summarizer at 10.202.50.251
10.202.50.251
09/28/2009 09:30:17
09/28/2009 17:30:17
09/24/2009 17:09:23
Summarize every:
Next Scheduled Run Time (mm/dd/yyyy hh:min):
Summarize Data Immediately:
Summarize Now
Syslog Deletion Schedule
Delete Syslog Data Daily at:
Delete Summarized Data For (mm/dd/yyyy):
Note:
* Unless a specific date is provided, deletion of old syslog/summarized data happens only at the scheduled time of the day specified above.
* Database maintenance jobs should be run after the completion of "Next Scheduled Archive Time" and "Delete Syslog Data Daily At" scheduled runs. See documentation for details.
Host Name Resolution Settings
Resolve Destination Host Names
Resolve Source Host Names
Periodic Crawling Interval
1440
(in minutes)
Update

2. Under Reports Data Summarization Interval, important information about the Summarizer is displayed. Use the **Summarize every** drop-down lists to specify how often in hours and minutes the ViewPoint Reporting Module should process syslog data and update summary information.
3. Click the **Update** button to the right of this field.
4. To specify the next summarization time, enter a date in the form mm/dd/yyyy in the **Next Scheduled Run Time** field, and select the hour and minute values from the drop-down lists.
5. Click the **Update** button to the right of this field.
6. To update the summary information now, click the **Summarize Now** button. SonicWALL ViewPoint will automatically process the latest information and make it available for immediate viewing.

Note This will not affect the normally scheduled summarization updates on ViewPoint.

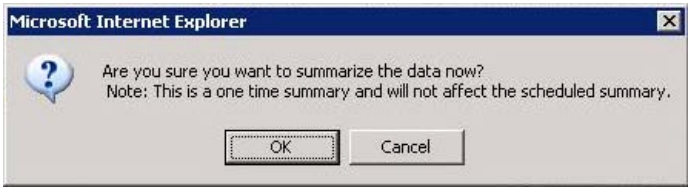
For more information about using and verifying the Summarize Now option, see the "Using Summarize Now" section on page 76.

Using Summarize Now

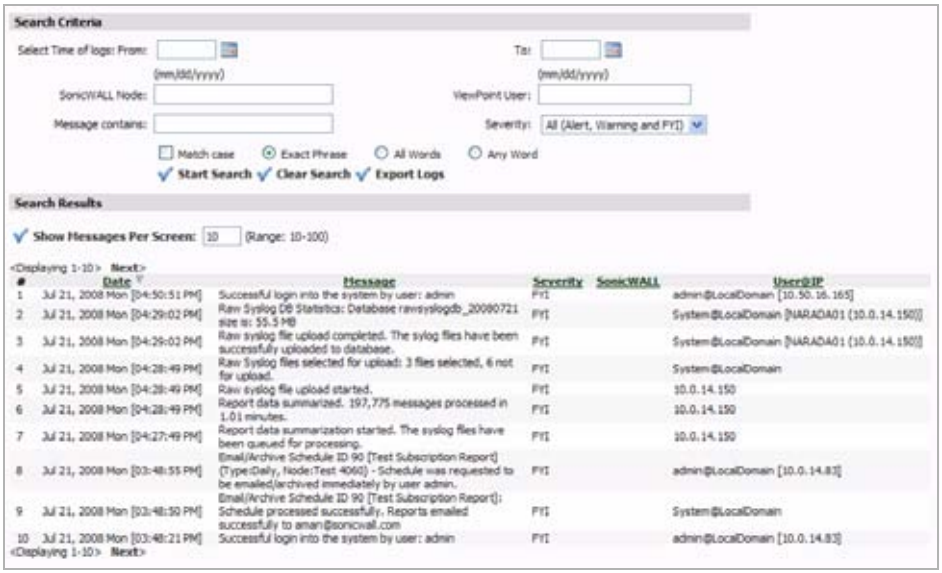
The Summarize Now feature allows the administrator to create instant summary reports without affecting the regularly scheduled summary reports. You can use Summarize Now to test that the Summarizer is gathering data for a managed unit. The SonicWALL ViewPoint Summarize Now feature is located in the **Console** tab under **Reports > Summarizer**. The SonicWALL ViewPoint Summarizer creates summary reports by default every 8 hours. Summary reports can be configured by the administrator to occur every 15 minutes to every 24 hours.

To use the Summarize Now feature, perform the following tasks:

1. Click the **Console** tab, expand the **Reports** tree and click **Summarizer**. Click the **Summarize Now** button.
2. You will see a pop-up window verifying that you want to summarize the data now. Summarizing data using **Summarize Now** is a one-time action and will not affect the scheduled summary. Click **OK** to continue.


Microsoft Internet Explorer
Are you sure you want to summarize the data now?
Note: This is a one time summary and will not affect the scheduled summary.
OK
Cancel

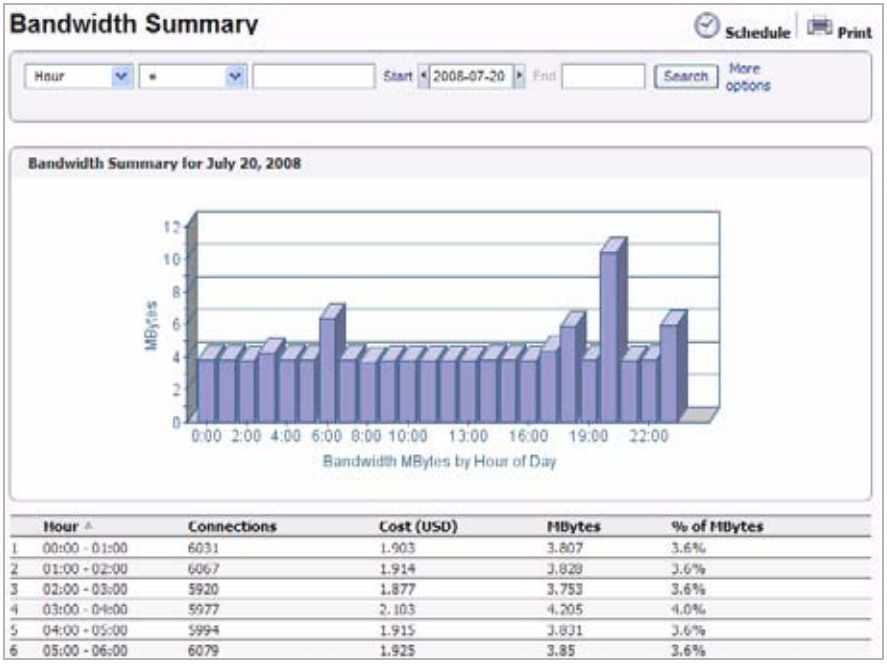
3. To verify summarization, navigate to **Log > View Log** in the left pane. Search for the message **Report Data Summarized** to verify that the Summarize Now action has completed.


Search Criteria
Select Time of logs: From:
To:
(mm/dd/yyyy)
(mm/dd/yyyy)
SonicWALL Node:
ViewPoint User:
Message contains:
Severity:
All (Alert, Warning and FYI)
Match case
Exact Phrase
All Words
Any Word
Start Search
Clear Search
Export Logs
Search Results
Show Messages Per Screen:
10
(Range: 10-100)
<Displaying 1-10> Next>
Date Message Severity SonicWALL User@IP
1 Jul 21, 2008 Mon [04:50:51 PM] Successful login into the system by user: admin FYI admin@LocalDomain [10.50.16.165]
2 Jul 21, 2008 Mon [04:29:02 PM] Raw Syslog DB Statistics: Database rawsyslogdb_20080721 size is: 55.5 MB FYI System@LocalDomain [NARADA01 (10.0.14.150)]
3 Jul 21, 2008 Mon [04:29:02 PM] Raw syslog file upload completed. The sylog files have been successfully uploaded to database. FYI System@LocalDomain [NARADA01 (10.0.14.150)]
4 Jul 21, 2008 Mon [04:28:49 PM] Raw Syslog files selected for upload: 3 files selected, 6 not for upload. FYI System@LocalDomain
5 Jul 21, 2008 Mon [04:28:49 PM] Raw syslog file upload started. FYI 10.0.14.150
6 Jul 21, 2008 Mon [04:28:49 PM] Report data summarized. 197,775 messages processed in 1.01 minutes. FYI 10.0.14.150
7 Jul 21, 2008 Mon [04:27:49 PM] Report data summarization started. The syslog files have been queued for processing. FYI 10.0.14.150
8 Jul 21, 2008 Mon [03:48:55 PM] Email/Archive Schedule ID 90 [Test Subscription Report] (Type:Daily, Node:Test 4060) - Schedule was requested to be emailed/archived immediately by user admin. FYI admin@LocalDomain [10.0.14.83]
9 Jul 21, 2008 Mon [03:48:50 PM] Email/Archive Schedule ID 90 [Test Subscription Report]: Schedule processed successfully. Reports emailed successfully to aman@sonicwall.com FYI System@LocalDomain
10 Jul 21, 2008 Mon [03:48:21 PM] Successful login into the system by user: admin FYI admin@LocalDomain [10.0.14.83]
<Displaying 1-10> Next>

4. When Summarize Now has completed, click the **UTM** tab at the top of the screen. In the left-most pane, click **MyReportsView** or click an appliance.

Note You may see incomplete data if you view the **Summary** section of a selected report before the **Summarize Now** process is complete. Wait for the **Report Data Summarized** message to be displayed in **Log > View Log**.

5. In the center pane, click a report to expand it, then click the **Summary** option underneath it. For example, click **Bandwidth**, then click **Summary** to review the summarized bandwidth usage data.



	Hour	Connections	Cost (USD)	MBytes	% of MBytes
1	00:00 - 01:00	6031	1.903	3.807	3.6%
2	01:00 - 02:00	6067	1.914	3.828	3.6%
3	02:00 - 03:00	5920	1.877	3.753	3.6%
4	03:00 - 04:00	5977	2.103	4.205	4.0%
5	04:00 - 05:00	5994	1.915	3.831	3.6%
6	05:00 - 06:00	6079	1.925	3.85	3.6%

6. Navigate to the Summary section of other reports in the center pane to see other summarized data.

Configuring the Syslog Deletion Schedule Settings

Syslog files sent from SonicWALL appliances are stored on the ViewPoint system, and are consolidated into the syslog database. The Summarizer processes the syslog data and stores the processed data in the summary database. After summarization and after the configured period of syslog storage, the syslog data can be periodically deleted from the system. This is necessary as the syslog files and database can consume a lot of space on the file system.

This section of the the Summarizer page also provides a way to delete summarized data for a certain date. For example, if summarized data is kept for a long time, such as 90 days, then you could use this option to remove some summarized data from a particular date within the 90 day period if the stored data was becoming too large.

Tip Run your database maintenance jobs soon after the completion of the scheduled tasks configured on this page for summarizing data and deleting old syslog data.

For information about setting the number of days to store syslog files, the syslog database, and the summary database, see the "Configuring Data Storage Settings" section on page 139.

ViewPoint requires large amounts of disk space for raw data storage. In previous versions, the maximum raw syslog database size was 2 GB. ViewPoint now provides enhanced database capacity by creating a new 2 GB database everyday. Each file name includes the date it was created for easy reference. Raw syslog data is used to create Custom Reports for UTM and SSL-VPN appliances.

To configure the syslog and summarized data deletion settings, perform the following:

1. On the **Console** panel, navigate to **Reports > Summarizer**.
2. Under **Syslog Deletion Schedule**, select the time for daily deletion in the hour and minute **Delete Syslog Data Daily at** drop-down lists. Syslog data will be deleted at this time only after being stored for the number of days configured.
3. Click the **Update** button to the right of this field.
4. To delete summarized data from a specific date, enter a date in the form mm/dd/yyyy in the **Delete Summarized Data For** field.
5. Click the **Update** button to the right of this field.

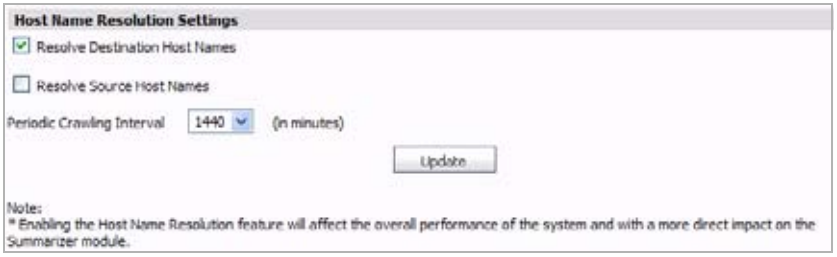
Configuring Host Name Resolution

The Host Name Resolution feature allows the administrator to enable and configure the time period for the name resolution crawler. The name resolution crawler periodically resolves host names for IP addresses found in reporting data. Once the host name is resolved, the name will appear in place of the IP address in reports that contain it. Over time, more host names will appear in the report data as they are added to the list.

The name resolution crawler runs by default every 24 hours (1440 minutes) and can be configured to run every 1 to every 60 hours.

To use the Host Name Resolution feature, perform the following steps:

1. On the **Console** panel, navigate to **Reports > Summarizer**. The Host Name Resolution Settings section is displayed at the bottom of the page.

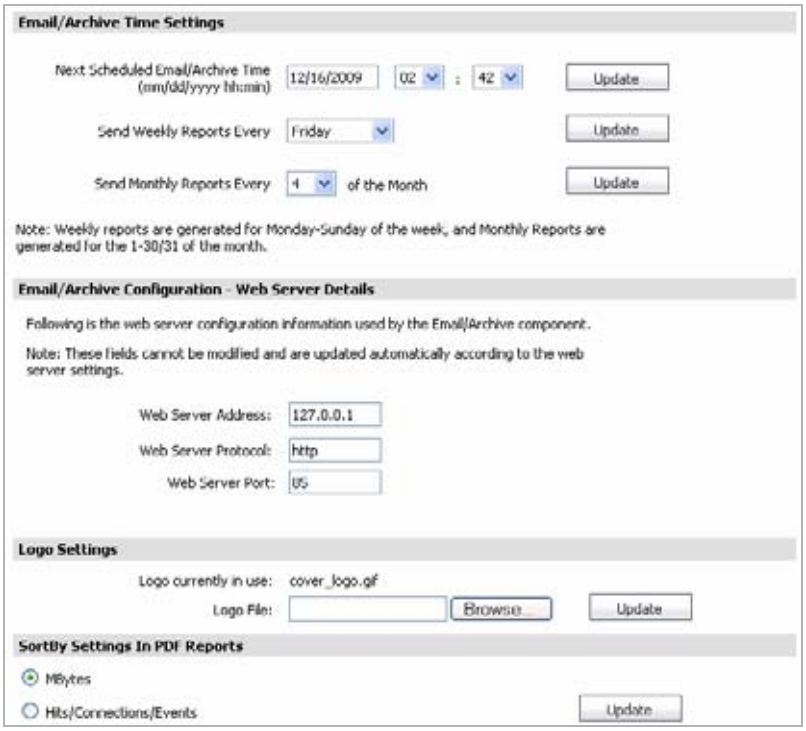

Host Name Resolution Settings
Resolve Destination Host Names
Resolve Source Host Names
Periodic Crawling Interval
1440
(in minutes)
Update
Note:
* Enabling the Host Name Resolution feature will affect the overall performance of the system and with a more direct impact on the Summarizer module.

2. To resolve host names for destination IP addresses, select the **Resolve Destination Host Names** checkbox.
3. To resolve host names for source IP addresses, select the **Resolve Source Host Names** checkbox.
4. To set the interval at which the name resolution crawler runs, select the number of minutes in the **Periodic Crawling Interval** drop-down list.

   Performance may be affected while the name resolution crawler is running, especially for the Summarizer module.

Email/Archive

The Console > Reports > Email/Archive page provides global options for setting the time and interval for emailing/archiving scheduled reports, and global settings for the Web server, logo, and PDF sorting options.



Configuring Email/Archive Settings

To configure Email/Archive and Web server settings, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Email/Archive**. The Email/Archive page displays.
2. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update**.
3. To specify the day to send weekly reports, select the day from the **Send Weekly Reports Every** list box and click **Update**.

4. To specify the date to send monthly reports, select the date from the **Send Monthly Reports Every** list box and click **Update**.
5. If the Web server address, port, or protocol has changed since SonicWALL ViewPoint was installed, the new values will automatically appear in the **Email/Archive Configuration** section. These settings can be modified on the System Interface, and cannot be modified here.
6. Under Logo Settings, you can select a logo to be used on reports. By default, the SonicWALL logo is used. To select another logo, click **Browse** next to the **Logo File** field or type the path and filename into the field, and then click **Update**.
7. Under SortBy Settings for PDF Reports, select one of the following as the sorting criteria for reports and then click **Update**.
   - **Mbytes** - Sort reports by the number of megabytes in each entry
   - **Hits/Connections/Events** - Sort reports by the number of hits, connections, or events, depending on the type of report

Scheduled Reports

The Scheduled Reports page allows you to manage all the report schedules in the system from a central location. This page lists all the schedules in the system, enabling you to monitor the status of these recurring schedules and re-send failed schedules, if needed. For information on adding a new scheduled report, see "Adding or Editing a Scheduled Report" section on page 135.

Under Search Results, the table indicates whether each schedule is enabled, along with information about the last execution time of a schedule, whether it ran successfully and the error that occurred if it failed, the last run type (scheduled or one time run), along with the node, owner and other relevant information.

The Summary section provides status information on your report schedules.

The Search Criteria section provides settings for searching report schedules. Results of your searches are displayed in the Search Results section.

To search for scheduled reports:

1. Click the **Console** tab, expand the **Reports** tree and click **Scheduled Reports**. The **Scheduled Reports** page displays.

Summary
Schedules in the system: 41
Next Scheduled Email/Archive Time: Jul 18, 2008 Fri [11:32 PM]
Weekly Schedules Last Attempted: Jul 14, 2008 Mon [11:32 PM]
Next Weekly Reports Time: Jul 21, 2008 Mon [11:32 PM]
Monthly Schedules Last Attempted: Jul 1, 2008 Tue [11:32 PM]
Next Monthly Reports Time: Aug 1, 2008 Fri [11:32 PM]
Search Criteria
Schedule Type: All
Status: All
SonicWALL Node: All
Owner: All
Name contains:
Error contains:
Use condition: AND
Match case:
Start Search
Clear Search
Search Results
Show Schedules Per Screen: 10 (Range: 10-100)
Go To Schedule Number:
<Displaying 1-10 of 41> Next>
ID Enabled Name Type Unit/Group/Device(s) Last Run (Local) Status Last Run
1 1 PrepaidAttackReports Daily PRO 2040 Mar 15, 2007 Thur [10:47 AM] SCHED
2 23 Network Activity For SonicWALL Daily TZ-170SPW Enh.11 Jan 24, 2007 Wed [01:56 PM] SCHED
3 27 Test for Int Inc Daily LogViewer View Jan 24, 2007 Wed [01:56 PM] SCHED
4 30 Web Daily LogViewer View Jul 17, 2008 Thur [11:32 PM] SCHED
5 37 Gateway-TZW PDF Report Test - Daily Daily Gateway-TZW Aug 14, 2006 Mon [10:37 PM] SCHED
6 39 engineering group report Daily MIT/Engineering/ Jul 17, 2008 Thur [11:35 PM] SCHED
7 40 Test For DB Leak Daily PRO 2040 Jun 2, 2008 Mon [11:30 PM] SCHED
8 45 Prepaid Test PDF Daily PRO 2040 Mar 15, 2007 Thur [10:48 AM] SCHED
9 46 VAR Networks Daily Report Daily TZ-170SPW Enh.11 Jul 17, 2008 Thur [11:36 PM] SCHED
10 47 4Feature Review Daily SSL-VPN
<Displaying 1-10 of 41> Next>
Select Only the 10 Schedules Displayed Above
Select All Schedules
E-Mail/Archive the selected schedules now
(Note: This is a one time event and will not affect the Scheduled E-Mail/Archive time.)
Delete the selected schedules
Re-send the selected schedules for dates (mm/dd/yyyy):
Report Date:
Report date to generate reports for. Used as beginning date for Weekly and Monthly reports.
End Date:
Applies to Weekly and Monthly reports. If omitted, end of week or month will be assumed.

2. Define the **Search Criteria** tab. The Search Criteria tab contains the following elements to refine your search:
   - **Schedule Type** - Select from the following schedule types:
     - –All Schedules
     - –Daily Schedules
     - –Weekly Schedules
     - –Monthly Schedules
   - **Status** - Select from the following status conditions:
     - –All

  - –Failed
  - –In Progress
  - –Success
  - –In Queue
  - –Partial Failure
- **SonicWALL Node** - Select from the following SonicWALL nodes:
  - –All
  - –Per Unit View
- **Owner** - Displays the owner (admin).
- **Name Contains** - Enter a context string to search by keywords.
- **Error Contains** - Enter a context string to search by keywords.
- **Use Condition** - Select from the following conditions:
  - –And
  - –Or
- **Match Case** - Select this checkbox to make your searches case sensitive.

3. Click **Start Search** to begin searching, or click **Clear Search** to reset all fields and start over.

The results of your search are displayed in a table in the Search Results section. You can adjust the number of schedules displayed, go directly to a row of the table, or navigate to other screens by clicking on links within the table.

To work with the search results:

1. To adjust the number of schedules displayed in the table, enter a number of rows to display in the **Show Schedules Per Screen** field, and then click on the checkmark.
2. To go directly to a row of the table, enter the row number in the **Go To Schedule Number** field, and then click on the checkmark.
3. The columns in the table are as follows:
   - The check box allows you select the schedule for emailing or archiving.
   - The notepad icon is a link to the Schedule Properties page.

- **ID** - The schedule ID number used to identify this schedule. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Enabled** - A green check mark indicates that this schedule is enabled, and a red X means that it is disabled.
- **Name** - The name of the report. Click on the highlighted report name link to access the report for editing. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Type** - All, Daily Schedules, Weekly Schedules, and Monthly Schedules.
- **Unit/Group/Devices(s)** - The host name of the SonicWALL appliance.
- **Last Run (Local)** - The date when the report was last generated. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Status** - Includes the following report status options:
  - **Blue**: Queued, waiting to be processed.
  - **Yellow**: Currently processing.
  - **Orange**: Report completed with errors.
  - **Red**: Report failed with errors.
  - **Green**: Report processed successfully.

  You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Last Run Type -** Indicates if the most recent run was a scheduled run or a one-time execution. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Last Error** - Displays the error condition from the most recent run, if any. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.

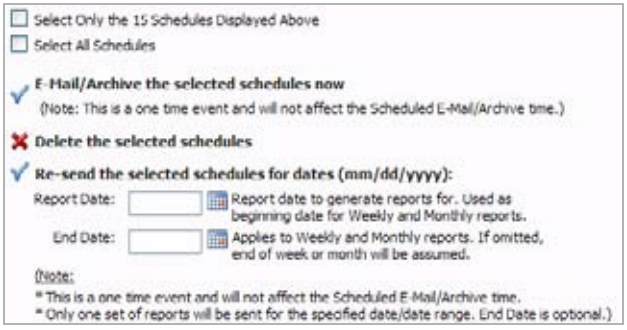
– **Owner** - Indicates the user ID of the user who created the schedule. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.

4. To view the properties for a schedule, click the notepad icon in that row. The Schedule Properties page displays.

5. To view the report, click on the name of the report. Your screen will change to the report screen on the UTM or SSL-VPN panel.

Resending Schedules

Apart from selecting multiple schedules for a one-time execution by selecting the appropriate checkboxes and clicking the **Email/Archive the Selected Schedules now**, you can re-send required schedules using the **Re-send the selected schedules for dates** option.


Select Only the 15 Schedules Displayed Above
Select All Schedules
E-Mail/Archive the selected schedules now
(Note: This is a one time event and will not affect the Scheduled E-Mail/Archive time.)
Delete the selected schedules
Re-send the selected schedules for dates (mm/dd/yyyy):
Report Date:
Report date to generate reports for. Used as beginning date for Weekly and Monthly reports.
End Date:
Applies to Weekly and Monthly reports. If omitted, end of week or month will be assumed.
(Note:
* This is a one time event and will not affect the Scheduled E-Mail/Archive time.
* Only one set of reports will be sent for the specified date/date range. End Date is optional.)

To resend any schedules, follow the procedures below:

1. Select the Schedule Type (Daily, Weekly, or Monthly) from the Search Criteria section and click **Start Search**. This lists all the schedules of the selected type. Select the checkboxes of the schedules you want to resend.

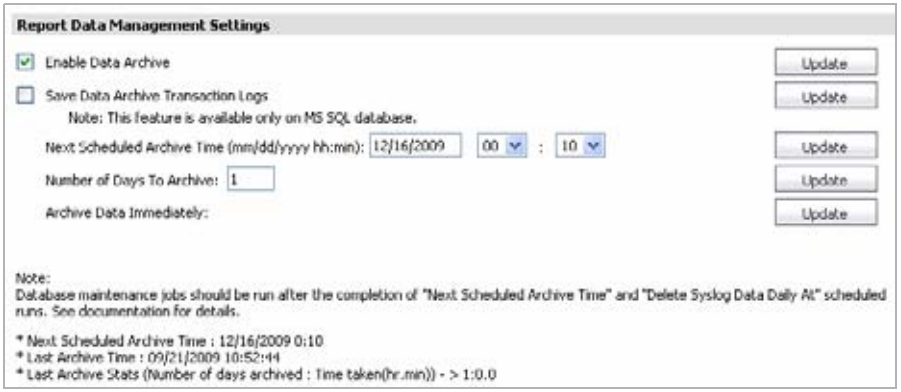
2. Provide a start date (and an end date if applicable). Reports are generated for the specified date/date range.

3. Click **Re-send the selected schedules for dates**. Reports are generated for the specific dates and emailed/archived as a one time option for all the schedules selected.

Management

Report Data Management allows the SonicWALL ViewPoint administrator to backup large amounts of report data incrementally and at specified intervals using MDTA. Typically, the total amount of data stored in an archive is equal to at least 30 days, although best benefits are seen when storing at least 60 days of summarizer data. MDTA allows this archive to be built over time, archiving as little as 1 day of data each time the MDTA process is run.

Note Total days to store summarized data in reports is set separately in the **Console > Reports > Summarizer** screen. Set this field for a value greater than 60 days for best results.


Report Data Management Settings
Enable Data Archive
Update
Save Data Archive Transaction Logs
Update
Note: This feature is available only on MS SQL database.
Next Scheduled Archive Time (mm/dd/yyyy hh:min): 12/16/2009 00 : 10
Update
Number of Days To Archive: 1
Update
Archive Data Immediately:
Update
Note:
Database maintenance jobs should be run after the completion of "Next Scheduled Archive Time" and "Delete Syslog Data Daily At" scheduled runs. See documentation for details.
* Next Scheduled Archive Time : 12/16/2009 0:10
* Last Archive Time : 09/21/2009 10:52:44
* Last Archive Stats (Number of days archived : Time taken(hr.min)) - > 1:0.0

Configuring Report Data Management

As an administrator, you choose the number of days worth of data to archive each time the MDTA process is run. With the exception of the current month, all available data is eligible for archiving. For example, if you specify 3 days as the number of days to archive, MDTA will archive 3 days of data, starting with the oldest available data and will repeat this process every day. In order to obtain optimal performance when viewing reports however, SonicWALL ViewPoint ensures that the current month is always kept in un-archived form.

Step 1 In the ViewPoint Administrator Interface, navigate to **Console > Reports > Management**.

Step 2 Check the box next to **Enable Data Archive** and click the corresponding **Update** button.

Step 3 Configure Data Archiving as follows, clicking the corresponding **Update** button after each line is completed:

Save Data Archive Transaction Logs	Select to save truncated data archive transaction logs during each MDTA operation. Click the **Update** button. This option is deselected by default in order to conserve disk space.
Next Scheduled Archive Time	Schedule an initial date (mm/dd/yyyy) and time (in 24-hour format) for the MDTA operation. Click the **Update** button. MDTA operations will take place every day at the time you specify, starting with your initial date selection.
Number of Days to Archive	Specify the number of days worth of data to consider for each MDTA operation.
Archive Data Immediately	Press this button to immediately start an on-demand MDTA operation. The archive will run immediately but your scheduled archive operation will still take place.

Note High-traffic systems can generate reports that consume large amounts of memory, disk space and CPU time when using MDTA. Set your **Number of Days to Archive** and **Scheduled Archive Time** accordingly. To view when MDTA operations are starting and how long the process is taking, navigate to the **Console > Log > View Log** screen and look (or search) for or “start” and “completed” times for “Report Data Archive.”

CHAPTER 9
Using Diagnostics

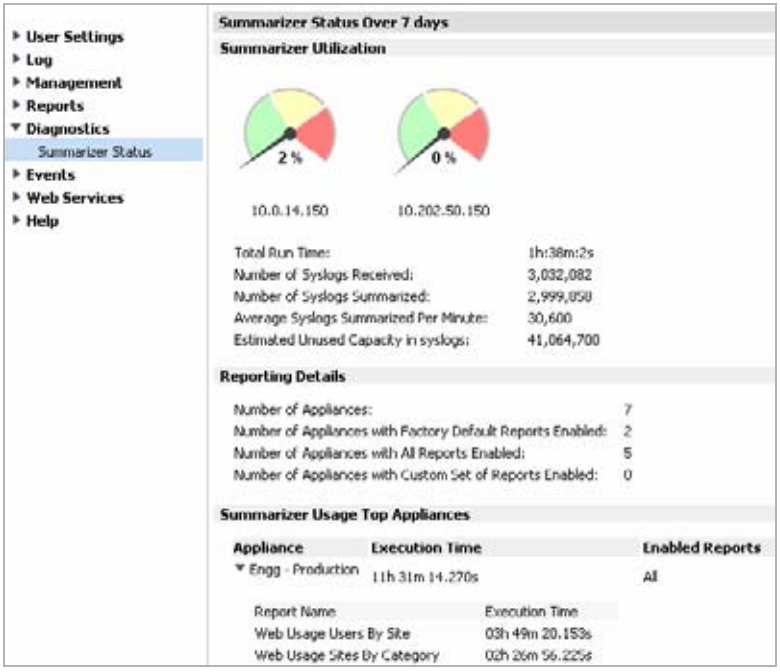
This chapter describes the diagnostic information that ViewPoint provides, including summarizer status information.

This chapter includes the following sections:

- "Summarizer Status" section on page 90

Summarizer Status

The **Summarizer Status** page displays overall summarizer utilization information for the deployment including database and syslog file statistics, and details on the current status of each summarizer.



The Summarizer Status screen provides performance metrics for your network administrator to plan, design, and expand your ViewPoint server deployment. This feature has information on the Syslog Collector and Summarizer metrics. The Summarizer metrics are available only for ViewPoint deployments that have Distributed Summarizer enabled (enabled by default on ViewPoint 5.1). The metrics are available for the past 24 hours, past seven days, and past 30 days.

These metrics are reset (to zero), every 24 hours for daily metrics, every seven days for weekly metrics, and every 30 days for monthly metrics. Weekly metrics are not shown unless the data collection for weekly metrics started earlier than the daily metrics. Similarly, monthly metrics are not shown unless data collection for monthly metrics started earlier than for daily and weekly metrics. ViewPoint will not display metrics for a component if the daily statistics collection started more than 26 hours earlier. This generally indicates that the component is not active.

You can receive alert emails when Summarizer Status shows any abnormalities.

To reach the Summarizer Status screen, navigate to the **Console** panel of ViewPoint and then to **Diagnostics > Summarizer Status**.

The Summarizer Status page is divided into a section showing the overall deployment-wide summarizer status and sections with details for each summarizer. See the following sections:

- Summarizer Status Over 7 Days, page 91
- Details for Summarizer at <IP Address>, page 93

Summarizer Status Over 7 Days

The Summarizer Status Over 7 Days section displays overall summarizer utilization information for the deployment including database and syslog file statistics. Results are calculated over the last 7 days, with historical data available over the last 30 days.

Summarizer Utilization

The top Summarizer Utilization section shows the average utilization of the summarizer over the applicable time period. The Dial Charts show the percent of total capacity used by the Syslog Collector or the Summarizer. The following metrics are also displayed in the Summarizer Utilization section:

Total Run Time: Total amount of time spent generating summarization statistical data and results over the applicable time period.

Number of Syslogs Received: Total number of syslogs received by the Summarizer over the applicable time period.

Note Not all syslogs are summarized – some syslogs, such as “heartbeat messages” are ignored. When **Web Event Consolidation/Home Port Reporting** is enabled, several syslogs may be ignored or alternatively, consolidated into a single syslog. If your appliance is managed by a different Agent, the results are not summarized here.

Number of Syslogs Summarized: Total number of syslogs summarized over the applicable time period.

Average Syslogs Summarizer per Minute: Average number of syslogs summarized per minute over the applicable time period.

Estimated Unused Capacity in Syslogs: The estimated remaining capacity of the summarizer in terms of the number of syslogs it can summarize, based on the time taken and number of syslogs summarized over the applicable time period. This number does not include the discarded syslogs.

Tip Usage Example: For this example, let's assume that the syslogs summarized per minute on a system is **18,108**, and the average number of syslogs received on that system is **91** per firewall, per minute. Divide the number of syslogs per minute (18,108) by the number of syslogs per appliance per minute (91). This yields an estimate of **198** security appliances, assuming that the current appliances are a fair sample of the security appliances on your network.
This simple math gives a reasonable estimate of the total number of security appliances this system should be able to handle, assuming that the Summarizer was to constantly summarize 24 hours (as in the case of a dedicated Summarizer).

Reporting Details

The Reporting Details section shows the number of appliances in the deployment, and the number with the following types of reports enabled:

- Factory default reports
- All reports
- Custom set of reports

Summarizer Usage Top Appliances

The Summarizer Usage Top Appliances section displays information about the appliances in the deployment that used the most summarizer time. Details are given about which reports were generated and their summarizer execution time.

Database Statistics

The size is displayed for each of the following databases:

- Current
- Archive
- Raw Syslog

Syslog File Storage Statistics

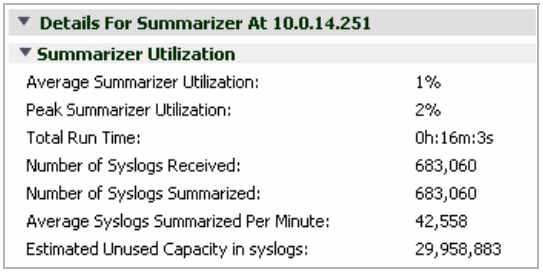
The size is displayed for each of the following syslog directories:

- Current
- Archived
- Bad

Details for Summarizer at <IP Address>

Summarizer Utilization

The Summarizer Utilization section for a specific summarizer shows the same information described above for the entire deployment, but only shows the values for this summarizer.


Details For Summarizer At 10.0.14.251
Summarizer Utilization
Average Summarizer Utilization: 1%
Peak Summarizer Utilization: 2%
Total Run Time: 0h:16m:3s
Number of Syslogs Received: 683,060
Number of Syslogs Summarized: 683,060
Average Syslogs Summarized Per Minute: 42,558
Estimated Unused Capacity in syslogs: 29,958,883

Reporting Details

The Reporting Details section shows the number of appliances serviced by this summarizer, and the number with the following types of reports enabled:

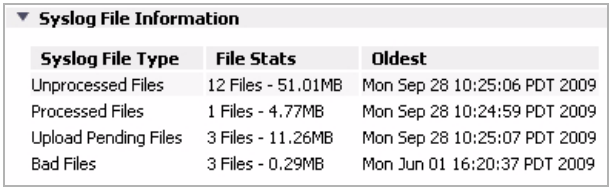
- Factory default reports
- All reports
- Custom set of reports

Summarizer Usage Top Appliances

The Summarizer Usage Top Appliances section displays information about the appliances serviced by this summarizer that used the most summarizer time. Details are given about which reports were generated and their summarizer execution time.

Syslog File Information

This section displays syslog file details for the selected summarizer.



Syslog File Information

Syslog File Type	File Stats	Oldest
Unprocessed Files	12 Files - 51.01MB	Mon Sep 28 10:25:06 PDT 2009
Processed Files	1 Files - 4.77MB	Mon Sep 28 10:24:59 PDT 2009
Upload Pending Files	3 Files - 11.26MB	Mon Sep 28 10:25:07 PDT 2009
Bad Files	3 Files - 0.29MB	Mon Jun 01 16:20:37 PDT 2009

The Syslog File Information table is divided into three columns:

- **Syslog File Type**: The type of files being reported on.

  There are ten main syslog file types:

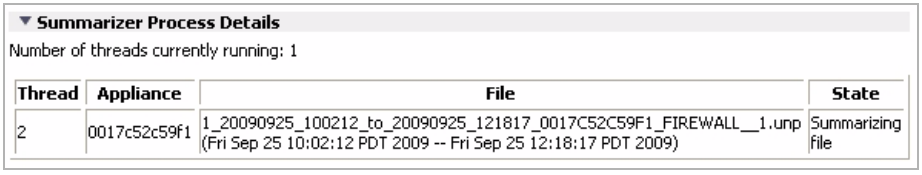
  – Processed Files
  – Unprocessed Files
  – Grouped Files
  – Not Mine Files
  – Infected Files
  – Archived Files
  – Bad Files
  – Upload Pending Files
  – Uploaded Files
  – Bad Upload Files

- **File Stats**: The number of syslog files in the category and their size in Megabytes.
- **Oldest**: The date and time on the oldest file in the category.

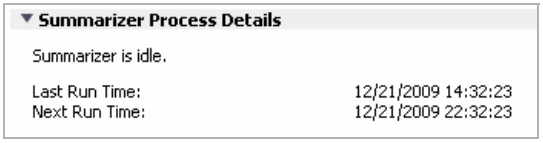
Summarizer Process Details

The Summarizer Process Details section shows what tasks the summarizer is performing at the moment the **Console > Diagnostics > Summarizer Status** page displays. Refresh your browser display or leave the page and return to it to update the information.

If the summarizer is currently running, the page displays the thread, appliance identifier, file being used, and state of the summarizer.



If the summarizer is currently idle, the page displays the last run time and next run time.



CHAPTER 10
Granular Event Management

This chapter describes how to configure and use the Granular Event Management (GEM) feature in a ViewPoint environment.

This chapter contains the following sections:

- "Granular Event Management Overview" section on page 97
- "Using Granular Event Management" section on page 99
- "Configuring Granular Event Management" section on page 101
- "Viewing Current Alerts" section on page 108

Granular Event Management Overview

Granular Event Management (GEM) provides a customized and controlled manner in which events are managed and alerts are customized and enabled. On the Console panel, GEM allows you to systematically configure each sub-component of your alert in order for the alert to best accommodate your needs.

The GEM alert has multiple sub-components, some of which have further subcomponents. It is not necessary to configure all sub-components prior to creating an alert.

- **Severities**: Severity is used to tag an alert as Critical, Warning, or Information. Severities are included within each Threshold. You can change the severity levels of the threshold elements listed on the Console > Events > Threshold page.

- **Thresholds**: A threshold defines the condition that must be matched to trigger an event and send an alert. Each threshold is associated with a Severity to tag the generated alert as critical, warning, or information.

  One or more threshold elements are defined within a threshold. Each threshold includes the following elements: an Operator, a Value, and a Severity. When a value is received for an alert type, the GEM framework examines threshold elements to find a match for the specified condition. If a match is found (one or more conditions match), the threshold with the highest severity containing a matching element is used to trigger an event.
- **Schedules**: You can use Schedules to specify the day(s) and time (intervals) in which to generate an alert. You can also invert a schedule, which means that the schedule is the opposite of the time specified in it. For example:
  - Generate an alert during weekdays only, or weekends only, or only during business hours.
  - Do not generate an alert during a time period when the unit, network, or database are down for maintenance.

What is Granular Event Management?

The purpose of Granular Event Management is to provide all the event handling and alerting functionality for ViewPoint. The ViewPoint management interface provides screens for centralized event management on the Console panel, including screens for Events > Threshold, Schedule, and Alert Settings. The panel also provides an Events > Alert Settings screen where you can enable or disable alerts.

You can enable or disable an alert at the global or unit level in ViewPoint. At the global level, the alert is then applied to all units. Whenever you add a new unit to ViewPoint, the alerts set at the global level are applied to the new unit.

How Does Granular Event Management Work?

The Granular Event Management framework provides customized event handlingfor specific alerts about database and database log size, and security service subscription licenses. For a list of the predefined alerts, see “Using Granular Event Management” on page 99.

Using Granular Event Management

For convenience and usability, a number of default settings are predefined for severities, schedules, thresholds, and alerts. You can edit the predefined values to customize the settings for thresholds and schedules. The predefined defaults for each panel and screen are as follows:

Table 1 GEM Predefined Default Objects

Panel	Screens	Predefined Default Objects
Console	**Events > Thresholds**	Unit Status
		Database Size Status
		Database Log Size Status (on MySQL DB only)
		Summarizer Utilization
		Summarizer Backed-Up Files
Console	**Events > Schedule**	**Schedule Groups:**
		• 24x7
		• Weekdays 24 hours
		• 8x5
		• Weekend
		Schedules:
		• Schedule: admin
		• Monday 24 hours
		• Monday business hours
		• Tuesday 24 hours
		• Tuesday business hours
		• Wednesday 24 hours
		• Wednesday business hours
		• Thursday 24 hours
		• Thursday business hours
		• Friday 24 hours
		• Friday business hours
		• Saturday 24 hours
		• Sunday 24 hours

Panel	Screens	Predefined Default Objects
Console	**Events > Alert Settings**	Database Info
		Database Size Status
		Database Log Size Status (on MySQL DB only)
		Summarizer Utilization Status
		Summarizer Backed-Up Files Status (on MySQL DB only)

About Alerts

The **Events > Alert Settings** screens are available in the Console and UTM panels. You can enable or disable alerts on these screens.

The GEM framework provides different types of alert types for the respective areas of the ViewPoint application:

- UTM panel: Alert settings for Reporting
- Console panel: Alert settings for the ViewPoint application

Table 2 GEM Alert Types

Panel location	Available Alert Types
Console	Date Base Info
	Database Size Status
	Database Log Size Status (on MySQL DB only)
	Summarizer Utilization Status
	Summarizer Backed-Up Files Status (on MySQL DB only)
UTM	Anti Virus License
	CFS License
	Warranty License
	Anti Spyware License
	Intrusion License

Configuring Granular Event Management

To set up the GEM environment after installing ViewPoint, start with the Events screens on the Console panel. You should examine the Threshold and Schedule screens and make any necessary configuration changes. Then you can enable alerts in the Events screens on the Console panel and UTM panel.

See the following sections:

- “Configuring Events on the Console Panel” section on page 101
- “Enabling or Disabling Alerts on the UTM Panel” section on page 107

Configuring Events on the Console Panel

In the Events screens on the Console panel, you can configure the frequency of subscription expiration and task failure notifications, as well as severities, thresholds, schedules, and alerts for handling events.

See the following sections:

- “Configuring Event Thresholds” on page 101
- “Configuring Event Schedules” on page 104
- “Enabling or Disabling Alerts on the Console Panel” on page 107

Configuring Event Thresholds

In the **Events > Threshold** screen, you can view existing event thresholds and configure their elements, and add custom thresholds. A threshold defines the condition for which an event is triggered. Predefined thresholds have names similar to predefined Alert Types. Each threshold can contain one or more threshold elements. An element consists of an Operator, a Value, and a Severity.

The following tasks are described in this section:

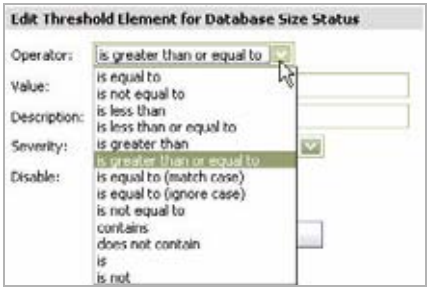
- “Editing an Event Threshold Element” on page 102
- “Enabling/Disabling Event Thresholds and Threshold Elements” on page 103

Editing an Event Threshold Element

To edit an existing element of a Threshold, perform the following steps:

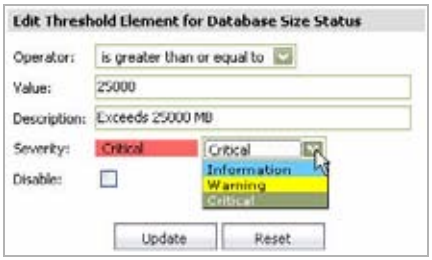
1. On the **Events > Threshold** screen, click the **Edit** icon located in the Configure column in the element row.
2. In the Edit Threshold Element window, you can edit the following fields:
   - Operator
   - Value
   - Description
   - Severity
   - Disable

3. In the **Operator** field, select from the drop down menu the type of operator to apply to your threshold element..



4. In the **Value** field, enter the value for your threshold element.
5. In the **Description** field, enter the description for your threshold element.

6. In the **Severity** field, select the severity priority from the drop down menu. These are color coded for your easy reference on the Events > Threshold screen.



7. To disable the threshold element, click the **Disable** check box. See "Enabling/Disabling Event Thresholds and Threshold Elements" section on page 103.
8. Click **Update**.

Enabling/Disabling Event Thresholds and Threshold Elements

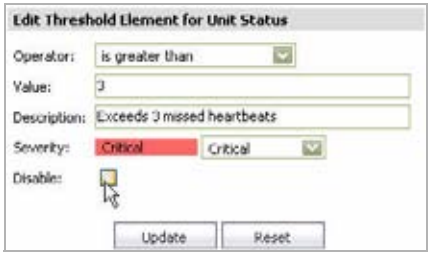
The GEM feature provides a **Disable** check box that allows you to disable or enable thresholds or individual elements within that threshold. If it is needed again, you can simply enable it.

You can disable a threshold by disabling all its elements. You can also disable individual elements within a threshold.

To enable or disable Thresholds and/or their elements, perform the following tasks:

1. On the **Console** panel, navigate to the **Events > Threshold** screen. On this screen, you are able to view existing Thresholds. You can also view existing elements within those thresholds by clicking the expand button by a threshold. You have the following two options for the enabling/disabling feature:
   - You can enable or disable a Threshold by disabling/enabling all the elements that exist within it.
   - You can enable/disable the individual elements within a Threshold.
2. To enable or disable a threshold and/or elements, click the edit button that is on the element level.

3. Select the **Disable** checkbox to disable the element or de-select the **Disable** checkbox to enable the element.



4. Click **Update**.

Configuring Event Schedules

The next component on the Console panel is **Events > Schedule**. In this screen, you can add, delete, or configure schedules and schedule groups.

Schedule groups are one or more schedules grouped within an object. Administrators and Owners can edit these objects. Other users should be able to view or use them only if the **Visible to Non-Administrators** check box is selected.

The following tasks are described in this section:

- "Adding an Event Schedule" on page 104
- "Editing an Event Schedule" on page 106
- "Adding an Event Schedule Group" on page 106
- "Deleting a Schedule or Schedule Group" on page 107

Adding an Event Schedule

In **Events > Schedules** you can add, delete, or configure schedules. You will see your schedules and schedule groups, their descriptions, and whether they are enabled. You can also individually delete one schedule or schedule group at a time by selecting the trash-icon on the right hand side for each row. For quick reference, you can hover your mouse over the descriptions to quickly view the type of schedule and the days and times when it is active.

To add an event schedule, perform the following steps:

1. On the **Events > Schedules** screen, click **Add Schedule**.
2. Select the **Visible to Non-Administrators** check box if you want the schedule to be visible and usable by non-administrators.
3. To temporarily disable a schedule, select the **Disable** checkbox.

4. Click **Invert** to create a schedule that is “off” during the dates and times that you specify.
5. In the Schedule field, you can create one or more schedules. For each schedule, configure either:

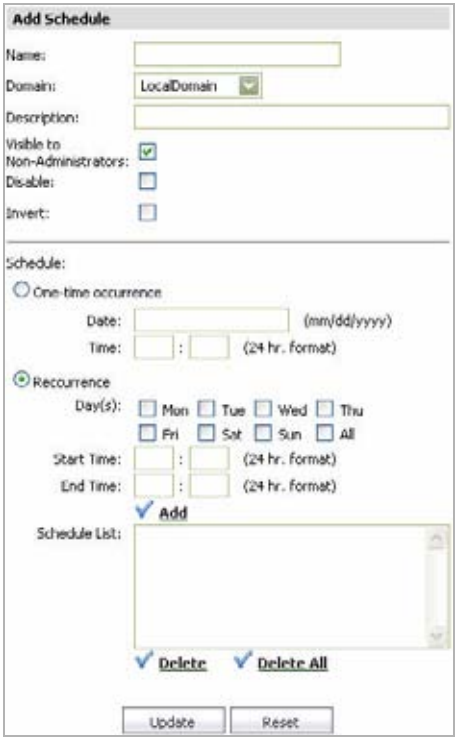
- **One Time Occurrence**

  –Fill in the **Date** and **Time** fields.

- **Recurrence**

  –Fill in **Days**, **Start Time**, and **End Time** fields.

6. Click **Add** to add this schedule to the **Schedule List** text box.



7. To delete an entry from the Schedule List text box, select the entry that you want to delete, and then click **Delete**. Click **Delete All** to delete all entries.
8. Click **Update** when you are finished.

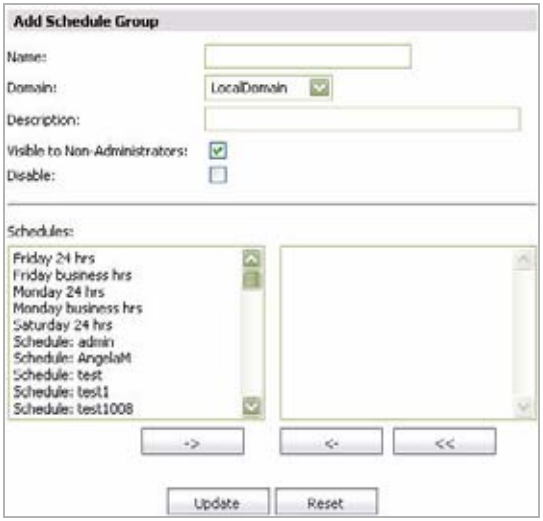
Editing an Event Schedule

To edit an existing schedule, click the **Edit** icon on the right side of the **Events > Schedule** screen. The screen and procedure for editing are the same as those for adding a schedule. See "Adding an Event Schedule" section on page 104.

Adding an Event Schedule Group

You can combine several schedules into a schedule group on the **Events > Schedule** screen. To add a schedule group, perform the following steps:

1. On the **Events > Schedule** screen, click the **Add Schedule Group** button.
2. Enter the name of your schedule group in the **Name** field.
3. Enter a description of your schedule group in the **Description** field.
4. Click the **Visible to Non-Administrators** check box to allow this schedule group to be viewed and used by non administrators.
5. Click the **Disable** check box to temporarily disable the schedule group.
6. In the **Schedules** field, select the schedule(s) to add to your schedule group, and then use the arrow buttons to move the selected schedule into or out of the group. To move multiple schedule groups and/or schedules all at once, hold the CTRL button on your keyboard while making your selections.



7. Click **Update**.

Deleting a Schedule or Schedule Group

You can delete schedules or schedule groups, or you can remove schedules from schedule groups.

To delete an event schedule, schedule group, or remove a schedule from a schedule group:

1. Navigate to the **Events > Schedule** screen.
2. Click the check boxes of the schedule groups or schedules that you want deleted. When you click the schedule group check box, the schedules within that schedule group will be deleted as well.
3. To remove a schedule from a schedule group, click the expand button on the schedule group, and select the schedules you wish to remove within that group.
4. To delete the selected schedule group(s) or remove the selected schedules from a group, click the **Delete Schedule Group(s)/Remove Schedules from Group** button.
5. To delete the selected schedule(s), click the **Delete Schedule(s)** button.

Enabling or Disabling Alerts on the Console Panel

The **Console > Events > Alert Settings** screen provides predefined alerts that apply to ViewPoint as a whole. You can hover your mouse over these to display information about them. You can enable or disable these alerts by selecting or clearing the checkbox in the **Enable** column for the alert.

Enabling or Disabling Alerts on the UTM Panel

You can enable or disable alerts for events pertaining to security services licenses on the UTM panel.To enable or disable an alert:

1. To enable an alert, select the checkbox under **Enabled** in the row for the alert.
2. To disable an alert, clear the checkbox under **Enabled** in the row for the alert.
3. Click **Enable/Disable Alert(s)**.

Viewing Current Alerts

You can view a list of current alerts on the **Events > Current Alerts** page of the panel. Select a global view or unit to view current alerts for your selection.

CHAPTER 11
Web Services

This chapter provides information about the Web Services feature. Web Services is a software system designed to support interoperability between ViewPoint and other network appliances, servers, and devices through an application programming interface (API).

Web Services is located in the Console panel of the ViewPoint management interface:

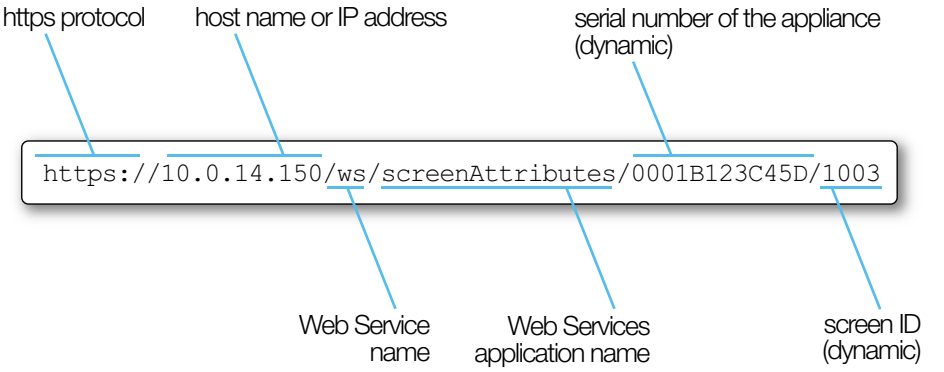
This chapter includes the following sections:

- "URI Basics" section on page 110
- "Settings" section on page 111
- "Status" section on page 112

URI Basics

The URI is a HTTPS string which is used to identify Web Services resources. Each URI is composed of both static and dynamic parts which differ based on each particular deployment.

The following provides a typical, though not comprehensive, URI example:



Note For more information on configuring and using Web Services in your deployment, download the *GMS Web Services Technote* at: <http://www.sonicwall.com/us/support.html>

Settings

The Settings screen allows configuration of a secure HTTPS Public URI for use with Web Services features. The public URI specified here is used to access Web Services and to ensure proper embedded cross-links between Web Services applications.

To configure Web Services Settings:

1. Navigate to the **Web Services > Settings** screen on the Console panel.

User Settings
Log
Management
Reports
Diagnostics
Events
Web Services
Settings
Status
Help
GMS Deployment
viewpoint 150
Select the deployment to configure Web Services for.
Public URI
Enter the public server name for this deployment. This name will be used to access Web Services on this server and will be included in embedded cross-links.
Note: The public server port is used to access GMS Web Services from the public domain. To modify the port on which GMS runs Web Services, please navigate to System Interface/Deployment/Settings
https://10.0.14.150:8445
(https://hostname[:port])
Update

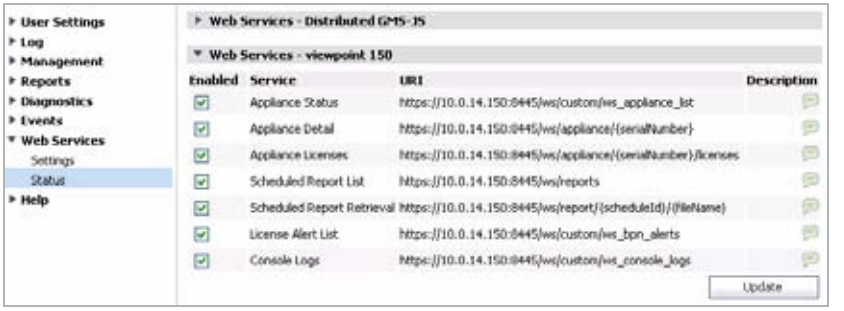
2. Choose which deployment you wish to configure from the drop-down list in the **GMS Deployment** section.
3. Enter the public server name and port in the **Public URI** section. This field is typically pre-populated during the ViewPoint install/setup process.
4. Click the **Update** button to save your changes.

Status

The status screen allows the administrator to view, enable, and disable individual Web Services across one or more ViewPoint deployments.

To view and configure Web Services status:

1. Navigate to the **Web Services > Status** screen on the Console panel.



2. Select or deselect the **Enabled** checkbox for the service(s) you wish to enable or disable.
3. Click the **Update** button to save your changes.
4. The Web Services table, in the **Web Services > Status** screen gives the following information about each Web Service:

Feature	Description
Enabled	If selected, this feature is currently enabled
Service	Indicates the name of the Web Service
URI	Indicates the full URI used to access this Web Service
Description	Provides a description of the Web Service

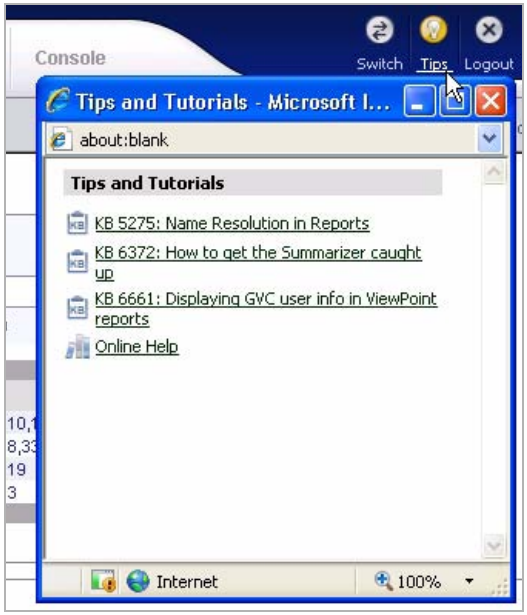
CHAPTER 12
Using ViewPoint Help

To access the ViewPoint online help, click the blue help button

in the top-right corner of the ViewPoint user interface.

Tips and Tutorials

Tips and tutorials are available in some pages of the user interface, and are denoted by a “Lightbulb” icon:



To access tips and tutorials:

1. Navigate to the page where you need help.
2. If available, click the Lightbulb icon in the upper right-hand corner of the window. Tips, tutorials, and online help are displayed for this topic.

About ViewPoint

The **Console > Help > About** page displays the version of ViewPoint being run, who the ViewPoint is licensed to, database information, and the serial number of the ViewPoint.

To access the ViewPoint online help, click the blue help button

in the top-right corner of the ViewPoint user interface.

CHAPTER 13
ViewPoint Reporting Features

This chapter describes how to use ViewPoint reporting, including the type of information that can appear in reports. A description of the available features in the user interface is provided. Settings for reporting on the Console panel are described.

This chapter includes the following sections:

- "ViewPoint Reporting Overview" section on page 115
- "Navigating ViewPoint Reporting" section on page 119
- "Showing Domain Names in Reports" section on page 130
- "Managing ViewPoint Reports on the Console Panel" section on page 131

ViewPoint Reporting Overview

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. ViewPoint Reporting complements SonicWALL's Internet security offerings by providing detailed and comprehensive reports of network activity.

The ViewPoint Reporting Module is a software application that creates dynamic, Web-based network reports. The ViewPoint Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWALL Internet security appliances. With ViewPoint Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs.

You can search saved reports by using the report search bar, available in most report screens in the ViewPoint UI. The search bar provides pre-populated quick settings for the search field, and a drop-down calendar for the start and end dates. The search operator field offers a comprehensive list of search operators that varies depending on the search field, which can be either text-based or numeric.

You can search all columns of report data except columns that contain computed values, such as %, Cost, or Browse Time. ViewPoint waits until you click Search before it begins building the new report.

The ViewPoint Reporting Module:

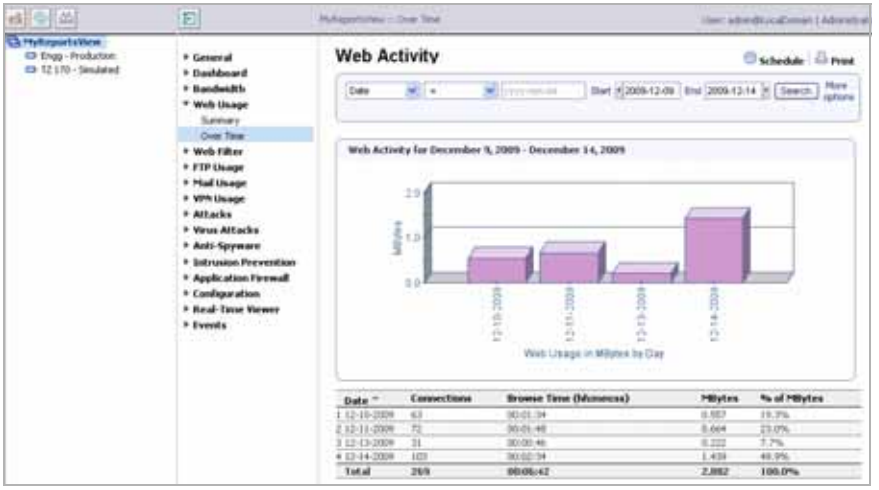
- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Tracks Web usage by users and by Web sites visited
- Provides detailed daily firewall logs to analyze specific events.

Note The ViewPoint Reporting Module receives its information from the stream of syslog data sent by each SonicWALL appliance and stores it in the SonicWALL ViewPoint database or as files on the hard-disk.

Viewing ViewPoint Reports

The ViewPoint reports are available on the **UTM** and **SSL-VPN** tabs of the ViewPoint interface:

The ViewPoint Reports view is divided into three panes:



- A list of individual units referred to as the TreeControl: In the left pane, you can select the top level view or a unit to display reports that apply to the selected view or unit. The top level view is **MyReportsView**.
- A list of reports: The middle pane provides a list of available reports that changes according to your selection in the TreeControl pane. The reports are divided into categories. You can click on the plus sign next to a category to view the list of reports in that category. You can click on an individual report name to view that report.

- The report: The right pane displays the report that you selected in the middle pane for the view or unit that you selected in the TreeControl. For most reports, the search bar is provided at the top of the pane. Above the search bar a link to the Scheduler is provided. You can change the time for the report to run by clicking the **Schedule** link or its clock icon in the upper right. A quick access link to your system's printer is also available in the upper right corner. To print the report, click the **Print** link or icon. To access the display settings for the report, click **More Options** to the right of the search bar.

The SonicWALL ViewPoint reporting feature provides the following configurable reports:

Table 3 Configurable Reports

General	Provides general unit and license status.
Dashboard	Provides a high-level activity summary.
Custom Report*	Provides Internet Activity and Website Filtering reports with details from raw data *Custom Reports are only available at the unit level.
Bandwidth	Provides bandwidth usage reports.
Services*	Provides events and usage by service protocol. *Services reporting is only available at the unit level.
Web Usage	Provides Web usage reports.
Web Filter	Provides web filter event reports.
FTP Usage	Provides FTP usage reports.
Mail Usage	Provides mail usage reports.
VPN Usage	Provides VPN usage reports.
Attacks	Provides attack event reports.
Virus Attacks	Provides virus attack event reports.
Anti-Spyware	Provides spyware event reports.
Intrusion Prevention	Provides intrusion event reports.
Application Firewall	Provides Application Firewall reports.
Authentication	Provides login reports.

Navigating ViewPoint Reporting

ViewPoint Reporting is a robust and powerful tool you can use to view detailed reports for individual SonicWALL appliances.

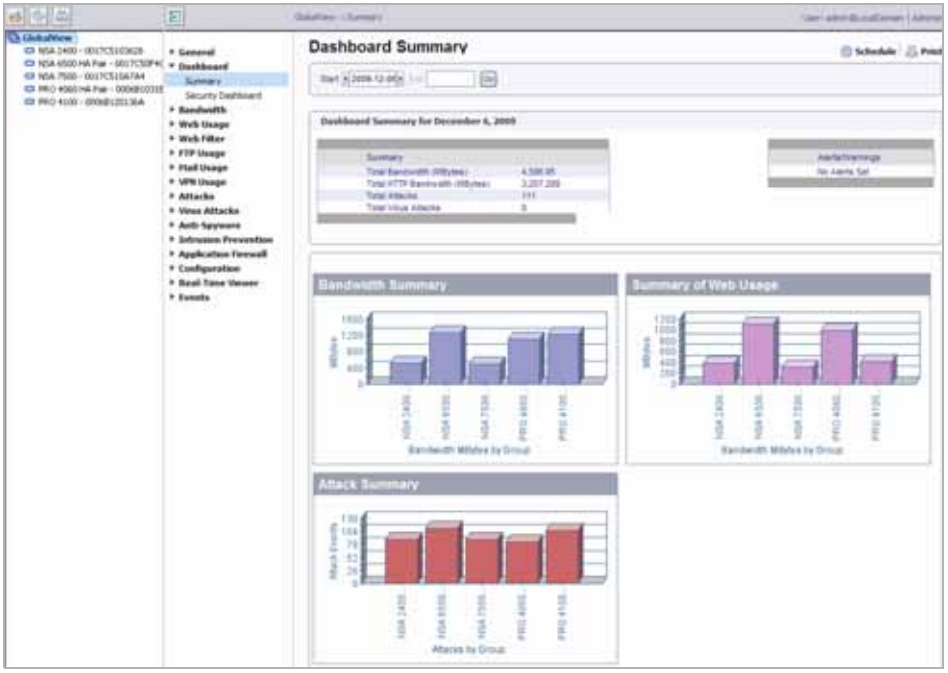
This section describes each view and what to consider when making changes. It also describes the Search Bar and display options for interactive reports, as well as other enhancements provided in SonicWALL ViewPoint . See the following sections:

- "Global Views" on page 120
- "Unit View" on page 121
- "Using Interactive Reports" on page 122
- "Searching for a Report" on page 123
- "Collapsible TreeControl Pane" on page 128
- "Enabling/Disabling Scheduled Reports" on page 128
- "Combined Reports" on page 128
- "Improved Navigation" on page 129

Global Views

From the Global view of the UTM Panel, Summary and Over Time reports are available for all SonicWALL appliances connected to SonicWALL ViewPoint.

To open the Global view, click the **MyReportsView** icon in the upper-left hand corner of the left pane. .



As you navigate the SonicWALL ViewPoint reports screens with the MyReportsView view selected and view different reports, the settings that you specify are maintained in effect throughout the session.

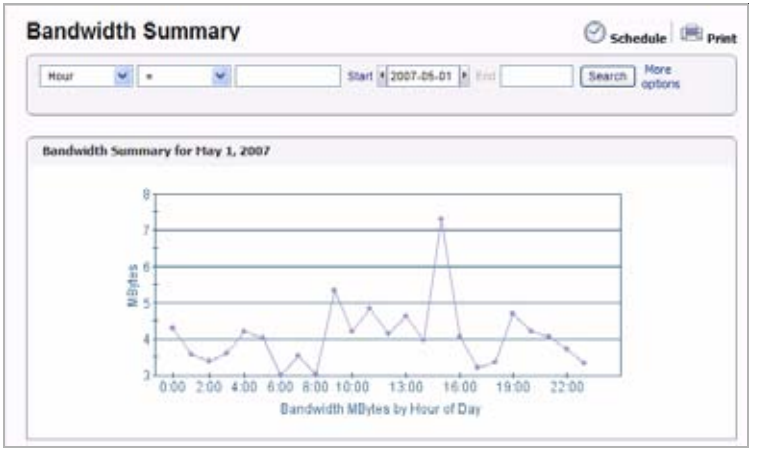
Unit View

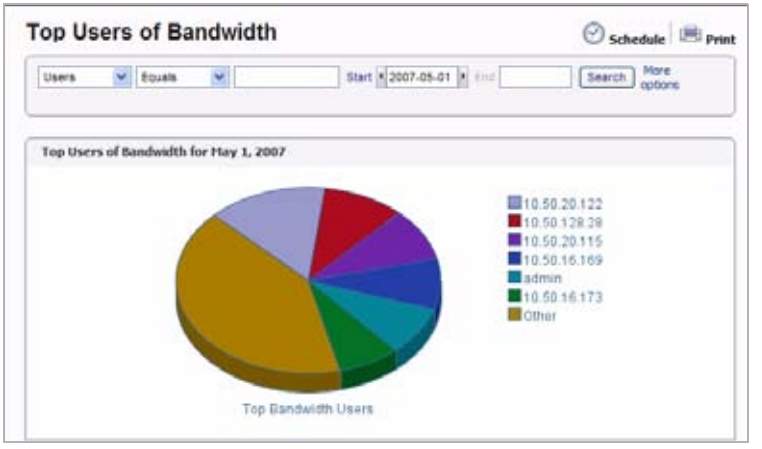
From the Unit view of the UTM panel, reports contain detailed data for the selected SonicWALL appliance. To open the Unit view, click the **UTM** tab. Then, click a SonicWALL appliance in the left pane of the SonicWALL ViewPoint interface. The report page for the SonicWALL appliance displays.

As you navigate the UTM panel with a single SonicWALL appliance selected and change settings, those settings will remain in effect throughout the session.

Using Interactive Reports

ViewPoint provides interactive reporting to create a clear and visually pleasing display of information. The following figures provide examples of an interactive report graph and a pie chart for Summary and Top Users. You can control the way the information is displayed by adjusting the settings which are collapsed in the search bar.





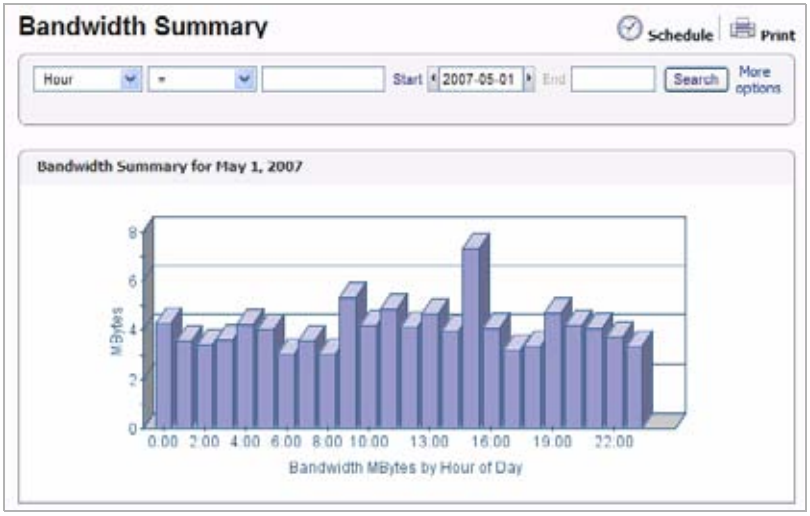
Searching for a Report

The search bar feature provides search and configuration capabilities for every report. In addition to the original quickset functions, the search bar has intuitive search fields to provide context-based searching.

The search bar contains a number of helpful components that allow you to specify search parameters and locate a report with ease. The components of the search bar include:

- A column drop-down list: The searchable column drop-down list contains all the searchable columns of a report. It is context-based, containing different options in different reports. The column drop-down list defines criteria for the search and filter functions.
- An operator drop-down list: There are two types of operator sets. If the content of the selected column is character-based, a character-based list is displayed. If the column contains numerical data, a list with mathematical symbols is displayed.
- A search text field: You can input a search string into this field.
- Start date and end date calendar fields: You can also search for reports by date. Clicking on the **Start** field displays a drop-down calendar where you can select day, month, and year by using the side arrows to navigate. You may also navigate through dates by clicking on the arrows located beside the **start date** and the **end date** fields.
- Detailed drop-down menu

The collapsed and expanded Search Bar views are shown below:



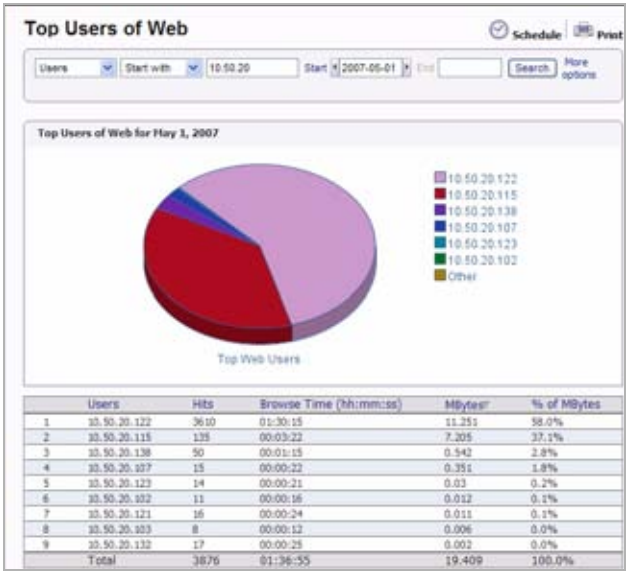
The search bar feature consists of a column drop-down list, an operator drop-down list, a search text field, and a detailed pull-down menu. Search/Filter functions can be performed by utilizing various components reporting at unit level.

The drop-down list contains all the searchable columns of a report. It is context-based, meaning that it contains different options in different reports. The column drop-down list defines criteria for search and filter functions to work on.

There are two different operator sets. If the content of the selected column is character-based, the character based operators will show:

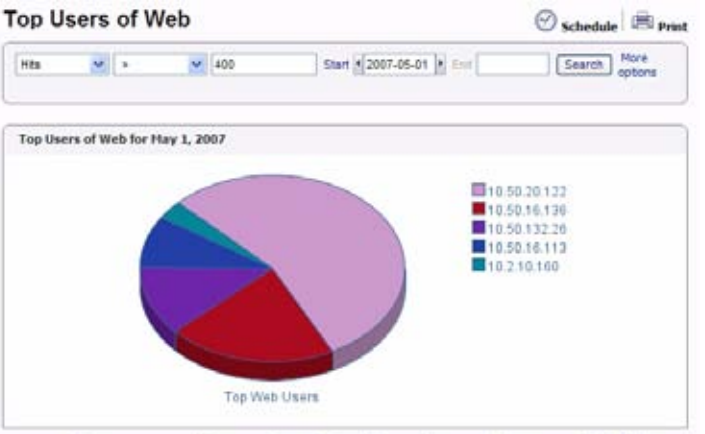
A character-based list contains **Equals**, **Start with**, **End with**, and **Contains** operators. If the content of the selected column contains numerical data, a list with mathematical symbols plus the **between** operator selection will display:

A generated report is shown below with user name (Users) starting with (Start With) “10.50.20” (the value of the search text field).



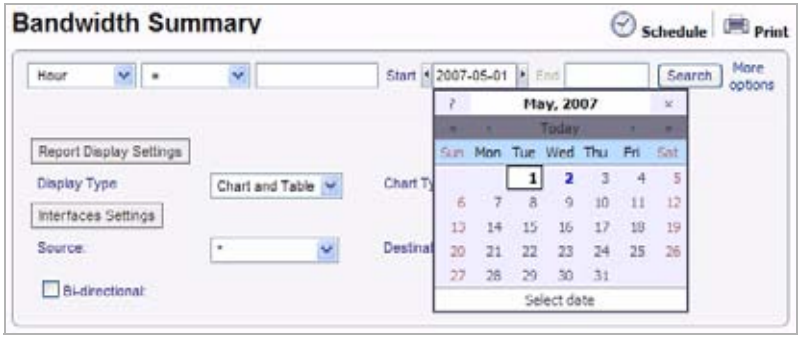
	Users	Hits	Browse Time (hh:mm:ss)	MBytes	% of MBytes
1	10.50.20.122	3610	01:30:15	11.251	58.0%
2	10.50.20.115	135	00:03:22	7.205	37.1%
3	10.50.20.138	50	00:01:15	0.542	2.8%
4	10.50.20.107	15	00:00:22	0.351	1.8%
5	10.50.20.123	14	00:00:21	0.03	0.2%
6	10.50.20.102	11	00:00:16	0.012	0.1%
7	10.50.20.121	16	00:00:24	0.011	0.1%
8	10.50.20.103	8	00:00:12	0.006	0.0%
9	10.50.20.132	17	00:00:25	0.002	0.0%
	Total	3876	01:36:55	19.409	100.0%

A generated report is shown below in which the Hit count (Hits column) is greater than (>) “100” (the value of the search field).



	Users	Hits	Browse Time (hh:mm:ss)	MBytes	% of MBytes
1	10.50.20.122	3610	01:30:15	11.251	54.9%
2	10.50.16.136	970	00:24:15	4.216	20.6%
3	10.50.132.26	2730	01:08:15	2.513	12.3%
4	10.50.16.113	537	00:13:25	1.84	9.0%
5	10.2.10.160	720	00:18:00	0.658	3.2%
	Total	8567	03:34:10	20.478	100.0%

The calendar module of the search bar is shown below. You can use the calendar module to easily select a date for the Start or End field. You can also manually type in a date. For single day reports, the End field is disabled.



The detailed options are “per report” based. For example, if you select “PIE” as the chart type for report A, you will still see Bar chart in report B if the bar chart was the existing chart type. The detailed drop-down menu can be expanded by clicking **More Options** as shown in the red circle below.

As Figure 1 and Figure 2 show, the options in the detailed drop-down menu are context-based. Figure 1 shows the detailed options of the “Web Usage By User” report. As you can see, Figure 2 contains different options because it is specific to the By User report.

Figure 1 Context-based Detail Options

Figure 2 Web Usage by User - Report Display Settings

Collapsible TreeControl Pane

The unit TreeControl pane can be collapsed to free up screen space by clicking on the the small arrow button to the right of the Add Unit, Modify Unit, Refresh, and Find buttons above the TreeControl pane. The panel can be brought back by clicking the same button.

Enabling/Disabling Scheduled Reports

ViewPoint allows you to disable a scheduled report without deleting it. This allows you to re-use the report at a later time without having to create it again. To enable or disable a report, navigate to the **Configuration > Scheduled Reports** page under the **UTM** tab. This screen shows all the scheduled reports on the current appliance. Select the checkbox in the row for a report(s) that you wish to disable, and click the **Disable Selected Scheduled Reports** button above the table. After confirmation, the check mark in the Enabled column is grayed out. To re-enable the report, use the **Enable Selected Scheduled Reports** button above the table.

Combined Reports

Users familiar with ViewPoint 4.0 will find two categories of reports that are no longer visible on the function tree: the **Browse Time** report and the **ROI** report. The information from these two reports have been folded into the **Web Usage** and **Bandwidth** reports, respectively. The **Web Usage** report pages now feature a **Browse Time** column. The **Bandwidth** report pages feature a **Cost($)** column that displays all the information previously displayed by the ROI reports.

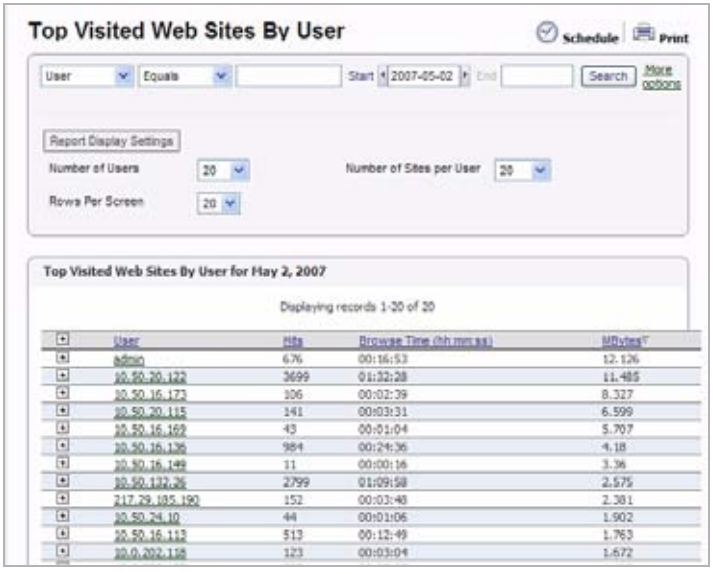
Improved Navigation

To save time, ViewPoint now features linked reports. **Web Usage** and **Web Filter** reports now link their **By User** and **By Site** pages. It is now possible to navigate directly from the **Web Usage > By User page** to a **Web Usage > By Site** page or from the **Web Filter > By User page** to a **Web Filter > By Site** page detailing the information of the site that the user has been browsing. Click the **Plus** sign next to the entry in the User column to show details, and hover the mouse over a site. A sticky tooltip will display with a link to the corresponding site's report page. This makes navigating from one report to the next much easier and makes retrieving detailed information simple.

Sample Navigation Use Case

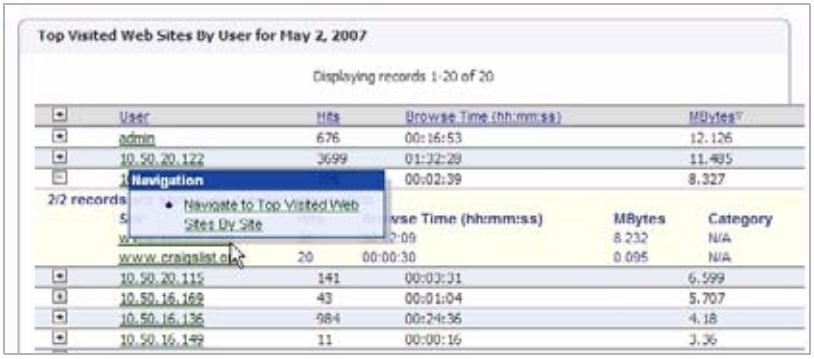
This sample use case demonstrates the improved navigation feature. In this use case you will open up the **Web Usage > By User** report and observe what sites the top browser has been visiting. Then you will move directly from the **By User** report to a detailed **By Site** report.

1. Navigate to the **Web Usage > By User** report from the **UTM** tab.



2. Click the **Plus** button next to any IP address in the User column. This displays detailed information about the sites that the user at that address has been visiting.

3. Hover your mouse over a site in this list. Click the **Navigate to Top Visited Web Sites By Site** link to navigate directly to the **Web Usage > By Site** report page.



The **Web Usage > By Site** report page shows detailed information about Web traffic to this site. Information in this report include the IP addresses of users who have browsed that site, as well as how much time they have spent browsing.

Showing Domain Names in Reports

Reports sometimes show the domain names of systems or websites, and sometimes show only the IP address. This is caused by different firmware versions on the appliances for which reports are being generated.

The reporting subsystem consumes the contents of src, dst, dstname, and other tags from the syslog messages. The syslog format and tags depend on the version of the firmware.

For firmware that includes name resolution, the reports will list the domain.

Note In SonicWALL ViewPoint 5.1 and above, the Name Resolution option on the UTM appliance (where the firmware supports it) is enabled when a unit is added. This does not apply to already existing appliances in the system.

Managing ViewPoint Reports on the Console Panel

There are management settings for the ViewPoint Reporting Module on the ViewPoint **Console** panel. The UTM panel contains limited configuration screens, used for managing scheduled reports and per-unit settings.The Reports section on the Console panel is divided into sections that allow you to manage system-wide settings, including the following:

Table 4 Console > Reports

Section	Settings
Settings	Report Settings/Options
	Log Viewer Settings
Summarizer	Summarizer Settings

Section	Settings
	Reports Data Summarization Interval
	Syslog Deletion Schedule
	Host Name Resolution Settings
Email/Archive	Email/Archive Time Settings
	Days to Store Archived/Published reports
	Email/Archive Configuration - Web Server Details
	Logo Settings
	SortBy Settings In PDF Reports
Scheduled Reports	Summary
	Search Criteria
	Search Results
Management	Report Data Management Settings

The Reports section of the Console panel controls settings for syslog data collection, summarizer configuration, email and archiving, scheduling reports, and archiving report data.

- For information about syslog data collection settings, see the "Enabling Report Table Sorting" section on page 72 in the Managing Reports in the Console Panel chapter.
- For information about the summarizer, see the following sections in the Managing Reports in the Console Panel chapter:
  - "About Summary Data in Reports" section on page 73
  - "Summarizer Settings and Summarization Interval" section on page 73
- For information about Email and Archiving settings, see the "Configuring Email/Archive Settings" section on page 81 in the Managing Reports in the Console Panel chapter.
- For a description of how to schedule reports in the Console panel, see the "Scheduled Reports" section on page 82 in the Managing Reports in the Console Panel chapter.
- For information about archiving report data using the Move Data to Archive (MDTA) feature, see the "Management" section on page 87 in the Managing Reports in the Console Panel chapter.

CHAPTER 14
Scheduling and Configuring Reports

This chapter provides information about scheduling automatic reports and configuring data summarization settings. It also contains instructions for configuring settings for the Dashboard > Summary report and describes how to view the list of current alerts on the **Events > Current Alerts** page. This chapter also describes how to export compliance reports in PDF format. The settings described in this chapter are applied on a per-unit basis.

This chapter includes the following sections:

- "Configuring Scheduled Reports" section on page 134
- "Selecting Reports for Summarization" section on page 137
- "Configuring Inheritance for Reporting Screens" section on page 138
- "Configuring Data Storage Settings" section on page 139
- "Configuring Summarization Data for Top Usage" section on page 140
- "Configuring Summarization Data for Bandwidth Reports" section on page 141
- "Configuring Dashboard Summary Reports" section on page 142
- "Viewing Current Alerts" section on page 144
- "Scheduling PDF Compliance Reports" section on page 144

Configuring Scheduled Reports

SonicWALL ViewPoint Reporting can automatically send reports to any email addresses that you specify. This section contains the following:

- "Viewing or Managing Scheduled Reports" on page 134
- "Adding or Editing a Scheduled Report" on page 135

To create scheduled email reports in PDF format as *Compliance Reports*, see the "Scheduling PDF Compliance Reports" section on page 144.

Viewing or Managing Scheduled Reports

To view , delete, or enable/disable currently scheduled reports, perform the following steps:

1. Click the **UTM** tab and select a SonicWALL appliance.
2. Expand the **Configuration** tree and click **Scheduled Reports**. The Scheduled Reports page displays.

3. On the Scheduled Reports page, to add a new scheduled report, click **Add Scheduled Report**. See "Adding or Editing a Scheduled Report" on page 135.
4. To edit a report, click the pencil icon in that row. See "Adding or Editing a Scheduled Report" on page 135.
5. To delete a report, select the checkbox in that row and then click **Delete Selected Scheduled Reports**.
6. To disable a scheduled report, select the checkbox in that row and then click **Disable Selected Scheduled Reports**.
7. To enable a disabled report, select the checkbox in that row and then click **Enable Selected Scheduled Reports**.
8. To select all reports in the list, click **Select All Scheduled Reports**.

Adding or Editing a Scheduled Report

You can add a new scheduled report or edit an existing one on the UTM panel on the Configuration > Scheduled Reports screen. When adding or editing the report, you can configure its name, category, formats, cover page, summary report page, and detailed reports page. You can also use or create a profile for the detailed reports page settings.

To add or edit a new scheduled report, perform the following steps:

1. Navigate to the Configuration > Scheduled Reports page and do one of the following:
   - To add a new schedule report, click the **Add Scheduled Report** button.
   - To edit an existing report, click the pencil icon in that row. The Scheduled Report Configuration window displays.
2. Enter a name for the report in the **Name** field.
3. Enter descriptive information in the **Description** field.
4. To email the report, select the **Email** check box. The screen expands to show email configuration settings.
5. Enter the IP address of the mail server into the **SMTP Server** field.
6. By default, the ViewPoint Reporting Module will use the email address that was configured in the Console panel in the Management > ViewPoint Settings screen as the Sender email address. To change it, enter a new Sender email address in the **Source Email Address** field.
7. Enter one or more destination email addresses, separated by semicolons, into the **Destination Email Addresses** field.
8. Enter the Subject Line that will appear in reports sent from the ViewPoint Reporting Module in the **Email Subject** field.
9. Enter text that will appear in the message body in the **Email Body** field.
10. To copy the contents of the report into the body of the email message, select the **Send Reports Inline** check box. To send the file as an email attachment, make sure this check box is deselected.

Note Reports can only be sent inline when all data is sent in a single report.

11. To archive the file on the server's hard disk, select the **Archive** check box and enter a path in the **Save Directory** field.

Specify the directory where the file will be archived in the **Save Directory** field.

12. For Report Type, select **Daily**, **Weekly**, or **Monthly**.
13. For Report Format, select **HTML**, **XML**, or **PDF**.
14. Select either **Include all data in a single report** or **Zip Reports into a single file**.
15. If you selected **PDF** for the Report Format, you can create a password to protect it by selecting **Password Protect the PDF File** and typing a password into the **Password** field. Users must input the password to view the contents of a password-protected PDF file. The content can be copied or printed, but is not editable by a PDF editor.
16. If the zip file is selected, you can create a password for it by selecting **Password Protect the Zip File** and typing a password into the **Password** field.

Note When both **PDF** and **Zip Reports into a single file** are selected, you can password-protect the PDF, but not the zip file.

17. For the Cover Page, enter a **Title** and **Subtitle** and select colors for the **Foreground** and **Background** of the cover page.
18. For Summary Report Page, you can select up to 4 reports. Select a report for the summary page from the **Choose the Summary Reports** drop down list, and then click **Add**.
19. For Detailed Report Page, do one of the following:
    - Click **Select an existing profile**, and then select the profile to use from the **Profile Name** drop-down list.
    - Click **Create a new profile**, type a profile name into the **New Profile Name** field, and then select the checkboxes in the Report list for each report to be included. You can click the checkbox next to the **Report** heading to select all reports in the list.
20. Optionally click **Configure Filters Options**. For this procedure see “Configuring Filters and Options” on page 137.
21. To see a preview of this scheduled report, click **PREVIEW**.
22. When finished, click **Add**.

Configuring Filters and Options

1. At the bottom of the Scheduled Report Configuration page, click the **Configure Filters/Options** button. The Display Options/Settings page displays.
2. Select the number of sites to display in Top Sites reports (default: 20).
3. Select the number of users to display in Top Users reports (default: 20).
4. Select the number of sites to display in Sites by User/Users By Site reports (default: 20).
5. Select the number of items to display in all other reports (default: 20).
6. Select the number of entries per item to display in all other reports (default: 20).
7. Under Inclusion Filter Parameters, enter a comma separated list of sites to include in By Site reports in the **Site List** field.
8. Enter a comma separated list of users to include in By User reports in the **User List** field.
9. To include the user's full name and IP address in the report, select the **Whole Name/IP** checkbox.
10. For Bandwidth Usage reports, select the source from the **Source Interface** drop-down list.
11. For Bandwidth Usage reports, select the destination from the **Destination Interface** drop-down list.
12. Click the **Update** button to apply changes. The new report will appear in the list on the Scheduled Reports page.

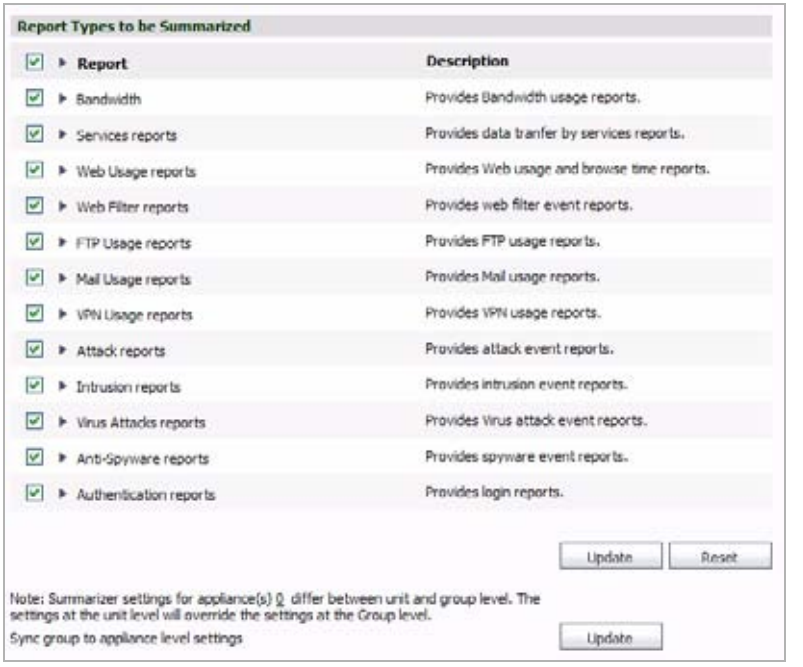
Selecting Reports for Summarization

This section describes how to tune the performance of the Summarizer by configuring which reports will be created. When an appliance is configured to communicate with ViewPoint, you need to prepare it for syslog data collection for reporting. Make sure the summarizer is collecting data for the reports you want for this unit.

To configure the Summarizer settings, perform the following steps:

1. Click the **UTM** tab.

2. Expand the **Configuration** tree and click **Summarizer Settings**. The Summarizer Settings page provides a list of reports and a correlating description of each report. Each report contains a checkbox that you can select to generate a summarized report.



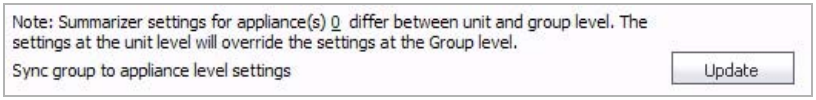
3. Select the checkbox of each report type to summarize.
4. When you are finished, click **Update**. Your configuration changes are saved automatically.

Configuring Inheritance for Reporting Screens

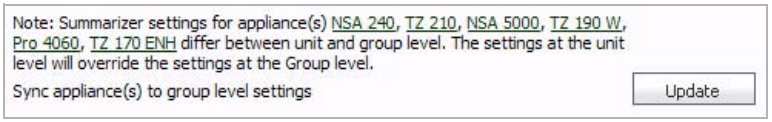
On the Configuration > Summarizer Settings screen, there is an option to synchronize report settings between the unit level and global level. This option can be displayed in any of the sections on this page when those settings are not synchronized between the unit level and global level.

This option provides inheritance support for report settings.

When you are viewing the screen at the unit level, the option is **Sync group to appliance level settings**. This is reverse inheritance. Click the **Update** button to apply your current unit level settings to the group to which this unit belongs.

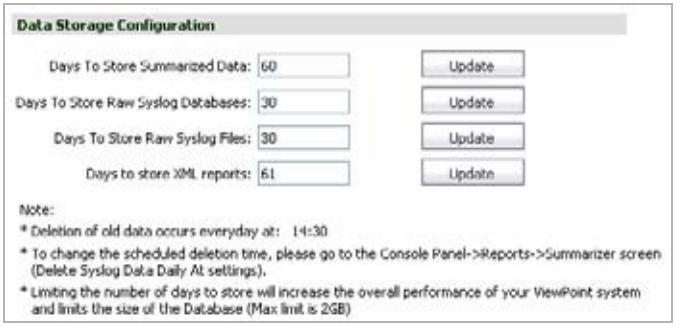

Note: Summarizer settings for appliance(s) 0 differ between unit and group level. The settings at the unit level will override the settings at the Group level.
Sync group to appliance level settings
Update

When you are viewing the screen at the global level, the option is **Sync appliance(s) to group level settings**. This is forward inheritance. Click the **Update** button to apply your current global level settings to the appliances in this group.


Note: Summarizer settings for appliance(s) NSA 240, TZ 210, NSA 5000, TZ 190 W, Pro 4060, TZ 170 ENH differ between unit and group level. The settings at the unit level will override the settings at the Group level.
Sync appliance(s) to group level settings
Update

Configuring Data Storage Settings

The Data Storage Configuration section of the **Configuration > Summarizer Settings** page allows you to specify the number of days to store summarized data and syslog data.


Data Storage Configuration
Days To Store Summarized Data: 60
Update
Days To Store Raw Syslog Databases: 30
Update
Days To Store Raw Syslog Files: 30
Update
Days to store XML reports: 61
Update
Note:
* Deletion of old data occurs everyday at: 14:30
* To change the scheduled deletion time, please go to the Console Panel->Reports->Summarizer screen (Delete Syslog Data Daily At settings).
* Limiting the number of days to store will increase the overall performance of your ViewPoint system and limits the size of the Database (Max limit is 2GB)

For all fields in this section, the minimum values should be 3 days, and will typically be longer.

Raw syslog data is transferred to the ViewPoint system by individual SonicWALL appliances, where it is stored in raw syslog files. The data from these files is combined and stored in a raw syslog database. Data from this database is processed by the Summarizer and then stored in the summarized data database.

The raw syslog files and databases older than the number of days specified here will get deleted by the global daily deletion schedule configured on the Console > Reports > Summarizer page. That page also provides a way to delete the summarized database for a certain date. See the "Configuring the Syslog Deletion Schedule Settings" section on page 78.

To configure the Data Storage Configuration settings:

1. On the **UTM** tab, expand the **Configuration** tree and click **Summarizer Settings**.
2. Scroll down to the **Data Storage Configuration** section.
3. Type the desired number of days to store summarized data into the **Days To Store Summarized Data** field and then click **Update**.
4. Type the desired number of days to store raw syslog database files into the **Days To Store Raw Syslog Databases** field and then click **Update**.
5. Type the desired number of days to store raw syslog database files into the **Days To Store Raw Syslog Databases** field and then click **Update**.
6. Type the desired number of days to store archived XML reports into the **Days To Store XML reports** field and then click **Update**.

Configuring Summarization Data for Top Usage

The Reports Summarization Data for Top Usage section of the Configuration > Summarizer Settings page allows you to enable Web event consolidation and resolve unrated categories.

When enabled, Web event consolidation reduces repetitive syslog event entries within the syslog database. Enabling Web Event Consolidation promotes search and summarizer efficiency by consolidating the syslog messages that result from a single click (for example, a visit to a Web page), and further correlates events by time proximity, such as multiple visits to the same URL by the same user within a set time, and HTTP header information. ViewPoint consolidates syslog messages under the main domain name.

When Web Event Consolidation is disabled, multiple syslog events are logged for one request. For instance, a single access to www.cnn.com can generate more than 70 syslog messages. Many of the 70 syslog messages refer to the links to other pages like images.cnn.com or video.cnn.com that are included in the Web page. In this simplified example, if **Domain Only** consolidation is

selected, then only one Web event is recorded (cnn.com). If **Host & Domain** is selected, then you would see three Web events. You would see all 70 Web events if consolidation was not enabled at all.

To enable Web event consolidation and resolve unrated categories, perform the following:

1. On the **UTM** tab, expand the **Configuration** tree and click **Summarizer Settings**.
2. Scroll down to the **Reports Summarization Data for Top Usage** section.
3. Select the **Enable Web Event Consolidation** checkbox to consolidate repetitive syslog event entries within the syslog database and then select one of the following levels of consolidation:
   - Host & Domain - More restrictive, less consolidation
   - Domain Only - More general, more consolidation
4. Optionally select the **Resolve "Not Rated" categories using message comparison** checkbox. If enabled, ViewPoint will attempt to categorize unrated items by comparing them to rated items, and will display the results in reports.
5. Click **Update**.

Configuring Summarization Data for Bandwidth Reports

The Reports Summarization Data for Bandwidth Reports section of the Configuration > Summarizer Settings page allows you to configure the currency type and cost per megabyte for use in bandwidth reports.

To configure the data for bandwidth reports, perform the following:

1. On the **UTM** tab, expand the **Configuration** tree and click **Summarizer Settings**.
2. In the **Reports Summarization Data for Bandwidth Reports** section, select the currency type in the **Type of Currency** field. Over 20 different currencies from around the world are available.
3. Specify an amount based on your chosen currency in the **Cost Per Mega Byte Bandwidth Use** field.
4. Click **Update**.

Configuring Dashboard Summary Reports

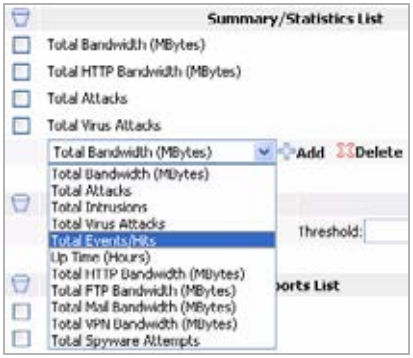
In the Configuration > Dashboard page, you can configure settings to control the information displayed by the Dashboard > Summary screen. Settings are available for the following:

- Summary statistics list at the top left of the Dashboard > Summary page
- Alerts list at the top right of the Dashboard > Summary page
- Reports list in the main body of the Dashboard > Summary page

To configure Dashboard Summary report settings, perform the following steps:

1. Click the **UTM** tab.
2. Expand the **Configuration** tree and click **Dashboard**.

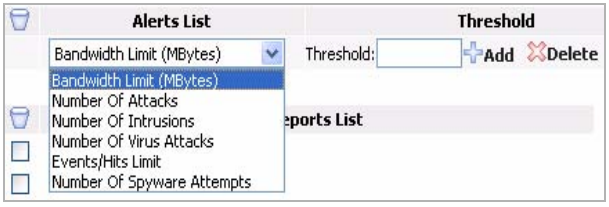
3. In the Summary / Statistics List section, to add a statistic to the Dashboard > Summary page, select it from the drop-down list and then click **Add**.



4. To remove a statistic from the Dashboard > Summary page, select the checkbox under the trashcan icon for that statistic, and then click **Delete**.

5. In the Alerts List section, to add an alert to the Dashboard > Summary page and to receive an email alert when the alert setting is matched, select an event type from the drop-down list, type a threshold value into the **Threshold** field, and then click **Add**.

   Alerts are emailed using the settings configured in the Console > Management screens. See “Settings” on page 61 and “Alert Settings” on page 64.



6. To remove an alert, select the checkbox under the trashcan icon for that alert, and then click **Delete**.

7. In the Reports List section, to add a report to the Dashboard > Summary page, select the report type from the drop-down list, and then click **Add**.

8. To remove a report from the Dashboard > Summary page, select the checkbox under the trashcan icon for that report, and then click **Delete**.

Viewing Current Alerts

You can view a list of current alerts on the **Events > Current Alerts** page of the UTM panel. Select a global view or unit to view current alerts for your selection.

Scheduling PDF Compliance Reports

ViewPoint can create scheduled email reports in PDF format. Called *Compliance Reports*, this feature allows you to export regular reports in universally readable format.

Compliance Report Overview

A *Compliance Report* is a report that collects report data and presents it in an organized format.

The ViewPoint Compliance Report feature allows administrators to provide more customized report summaries and to create more formal and defined layout of report information in PDF format. This feature provides the following benefits:

- Customizable cover page (Default also available)
- Customize Summary/ Descriptions for the reports.
- Ability to customize a set of reports.
- Three reports can be persisted as a profile so that it can be consumed by less experienced users in the system.
- Reports can be generated in industry standard PDF format.
- Compressed format provides a smaller sized file than an equivalent HTML report.
- The print quality is higher.

- This feature has the ability to open a 200 page PDF report with ease. In comparison, opening the same report in HTML takes a more extensive amount of time using IE, as it is weighed down by memory and other systems.

Requirements

Adobe Reader ® plug-in is required for the preview function.

How Do Compliance Reports Work?

ViewPoint has the capability to generate both online and scheduled reports in HTML format. Since PDF has become a standard document format for distribution, the compliance reports are based on this universal standard. Moreover, users are able to customize/define sections throughout the report. For example, they can assign different logos/titles to the cover pages for their customers.

Adding a New Scheduled Compliance Report

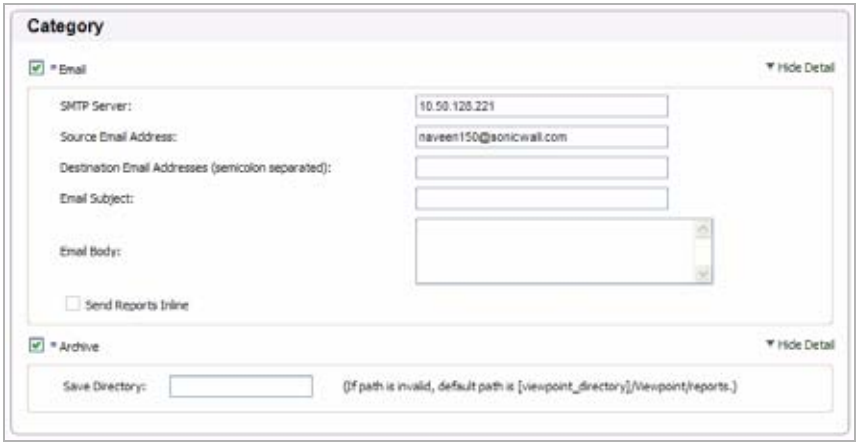
This section includes the following sub-sections:

- "Customizing Your Cover Page" section on page 147
- "Customizing Your Summary Report Page" section on page 148
- "Customizing Your Detailed Reports Page" section on page 149
- "Editing Existing Profiles" section on page 150
- "Verifying User Compliance Reports Configuration" section on page 152

To begin creating a new customized Compliance Report, perform the following steps:

1. Navigate to **UTM > Configuration > Scheduled Reports.**
2. Click the **ADD** button, to add a scheduled report.
3. The Scheduled Report Configuration page displays. In the **General** section, enter the name of your report into the **Name** field, and the report description.

4. In the **Category** section, select the **Email** check box. The details window displays:
   - **SMTP Server** field: Enter your SMTP Server IP address or hostname.
   - **Source Email Address** field: Enter your Source Email Address.
   - **Destination Email Address** field: Enter the Destination Email Address(es).
   - **Email Subject** field: Enter your Email Subject.
   - **Email Body** field: Enter your Email Body.

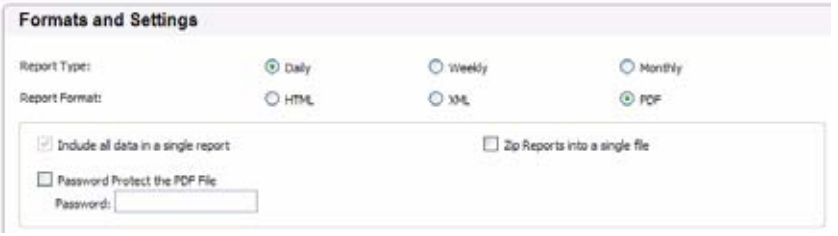


5. To archive a directory, click the **Archive** check box. Enter the your desired directory you want to archive into the **Save Directory** field.

To change the format and settings of your customized compliance report, perform the following steps:

6. In the **Format and Settings** category, select the **Report Type** that reflects the time interval you want to view your reports, either **Daily**, **Weekly**, or **Monthly**.

7. Select the PDF report format in the **Report Format** category. Selecting the **PDF** option will open additional fields to allow you to customize the set up of the **Cover Page**, **Summary Report Page**, and **Detailed Report Page** of your report in PDF format.



8. To zip all of your reports into a single file, select the check box next to the **Zip Reports into a single file** check box.

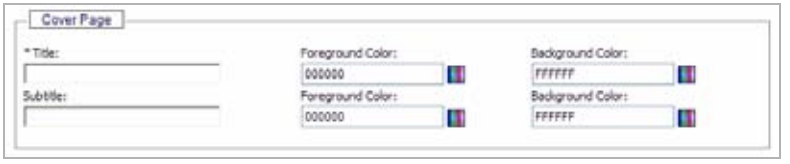
Note PDF will disable some options that are only applicable to HTML.

9. For custom reports, enter the template folder name into the **Template Folder Name** field.

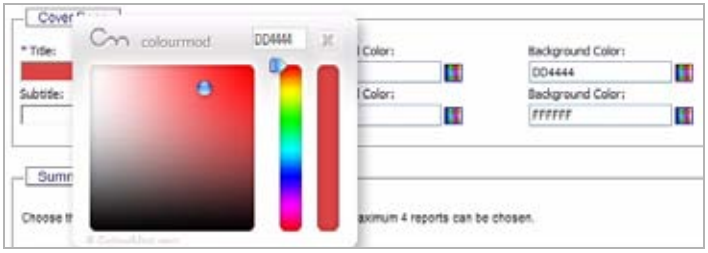
Customizing Your Cover Page

The Cover Page section allows the user to design a cover page for their report using different color schemes.

1. **Title** field: Enter the document title.
2. **Subtitle** field: Enter the document subtitle. (Optional).



3. Select the color for the Title and Subtitle's foreground and background by clicking the gradient color box in the right side of the each field. You may select a color by either choosing a color on the color bar and then selecting its value in the color box or by typing in the HTML color.

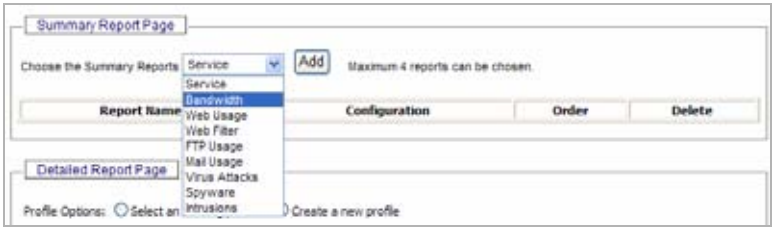


4. The color codes are automatically filled in the corresponding fields once the color chooser window is closed.

Customizing Your Summary Report Page

The Summary Report Page allows you to add new reports and individually customize their appearance.

1. On the Summary report page, select the type of summary reports you need, up to a maximum of 4 reports. Then, click the **Add** button. The report will be created based on the type of summary report you have selected.
2. Enter the report title in and report description in the appropriate fields.
3. Select the text color for the title and description.
4. Select the background color for both fields.
5. Select the order in the **Order** drop-down window.

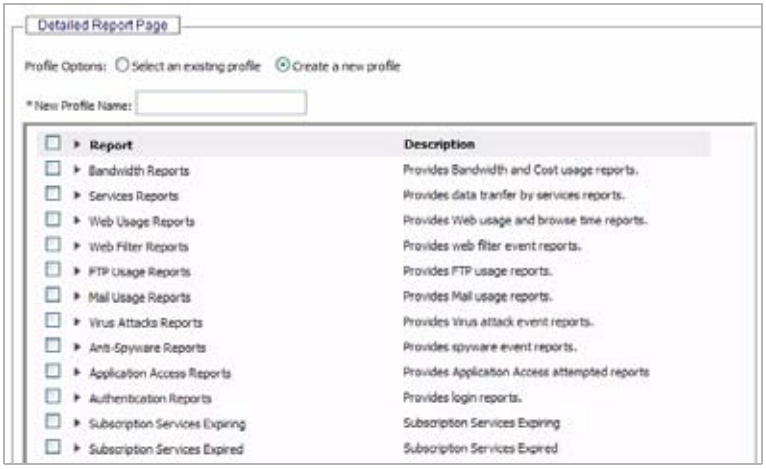


6. You may continue to add reports based on the summary you select in the Summary Reports drop-down menu. Repeat steps 1-5 to add more summary reports.

Customizing Your Detailed Reports Page

The Details Report Page provides you with a list of reports you may select to include in your report summaries. You can refine your setting for your report in more detail in the Detailed Report Settings category. First, select the appropriate profile setting for your report. If you are creating a new profile, select the **Create a New Profile** button.

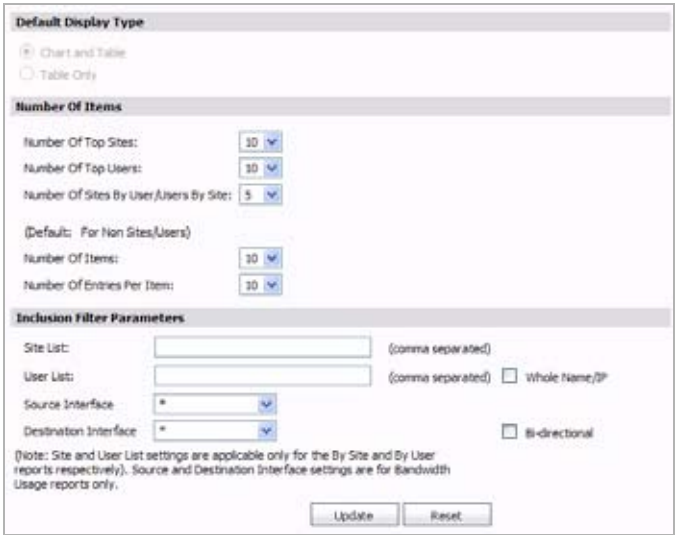
1. **New Profile Name** field: Enter the name of your new profile.



2. To determine the type of reports that will be summarized in your compliance report, check the boxes next to the reports you need. Sub-folders are revealed to each folder by clicking the plus icon. When all sub-folders are selected, the main folder will be selected.
3. When you have completed your selection(s) of reports, scroll down the page until you see a check button with Configure Filters/Options beside it. Click the check mark button.

Configure Filters/Options
(Note: You can set filters and display options to be applied for reports in this schedule here).
Add
Cancel
Preview

4. In the Configure Filter/Options section, you are able to decide how your filter and display is set. Once you have clicked the check button, fill out the table accordingly.


Default Display Type
Chart and Table
Table Only
Number Of Items
Number Of Top Sites:
Number Of Top Users:
Number Of Sites By User/Users By Site:
(Default: For Non Sites/Users)
Number Of Items:
Number Of Entries Per Item:
Inclusion Filter Parameters
Site List:
User List:
Source Interface
Destination Interface
(comma separated)
Whole Name/IP
Bi-directional
(Note: Site and User List settings are applicable only for the By Site and By User reports respectively). Source and Destination Interface settings are for Bandwidth Usage reports only.
Update
Reset

Editing Existing Profiles

A profile is associated with selected reports from the report list. You have the ability to go back and edit existing profiles in your scheduled reports. Since the report list is populated based on the report type selection, a profile is associated with the report type also. Instead of three categories, there will only be two: **single day** or **multi-days**. A profile in a single report will not be seen be seen by the users when they select weekly or monthly as report types.

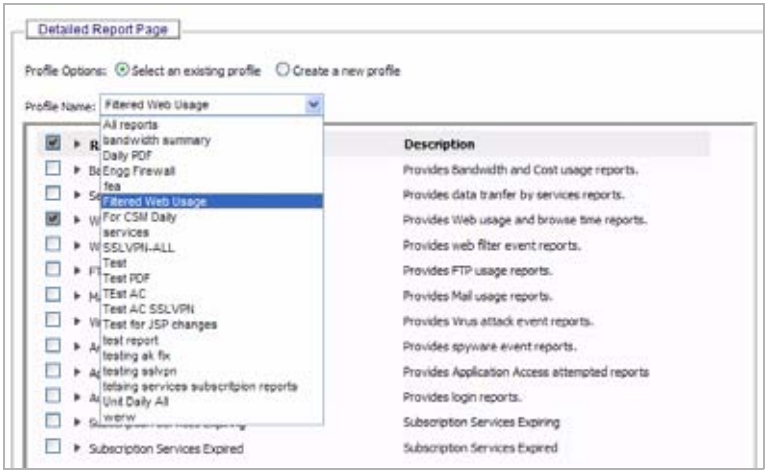
To edit existing profiles, perform the following tasks:

1. Click the **Edit** icon, located next to the report name you want to edit.

2. In the Detailed Page section, choose the **Select an existing profile** button.

Note You are able to delete an existing profile in that section by clicking the **Delete Selected Scheduled Reports** button located at the top of the page.

3. From the drop-down list in the Detailed Report Page, select the profile name you wish to edit. Choose the reports you want to add or remove from that profile. If a new profile has the same name as one of the existing profiles, the behavior will be the same as users opening the existing profile and edit the report list. When selecting an existing profile, the associated reports are checked in the report list automatically.



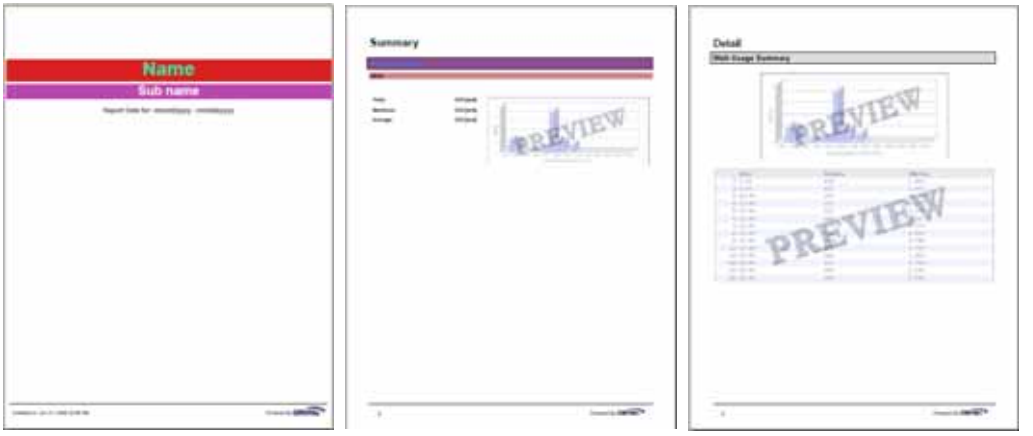
A default cover page is provided:

Verifying User Compliance Reports Configuration

If you have chosen the PDF version of this report, you now have the option to see a preview of the report covers you have created and how all of the report summaries you added will fit into that template.

To review your customize PDF settings, click the **Preview** button:

Figure 3 Cover page; Summary page; and Details page Preview



Note The images used for the preview do not use actual data.

CHAPTER 15
Viewing Reports

This chapter describes how to generate reports using the SonicWALL ViewPoint Reporting Module.

The following section describes how to configure the settings for viewing reports:

- "Managing Report Settings" section on page 154

Select from the following reports:

- "Viewing General Status Reports" section on page 157
- "Viewing Dashboard Reports" section on page 159
- "Using Custom Reports on UTM Appliances" section on page 163
- "Viewing Bandwidth Reports" section on page 180
- "Viewing Services Reports" section on page 189
- "Viewing Web Usage Reports" section on page 191
- "Viewing Web Filter Reports" section on page 209
- "Viewing File Transfer Protocol Reports" section on page 225
- "Viewing Mail Usage Reports" section on page 231
- "Viewing VPN Usage Reports" section on page 238
- "Viewing Attacks Reports" section on page 250
- "Viewing Virus Attacks Reports" section on page 260
- "Viewing Anti-Spyware Reports" section on page 266

- “Viewing Intrusion Prevention Reports” section on page 273
- “Viewing Application Firewall Reports” section on page 281
- “Viewing Authentication Reports” section on page 287
- “Viewing the Log” section on page 290

Managing Report Settings

All of the reports in ViewPoint report on data gathered on a specific date or range of dates. You can also edit the report settings for each report by using the Search Bar and the More Options button.

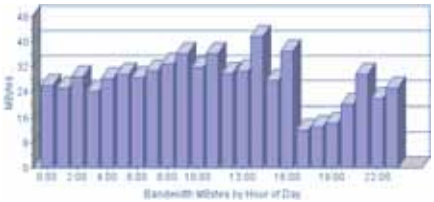
Editing Report Settings

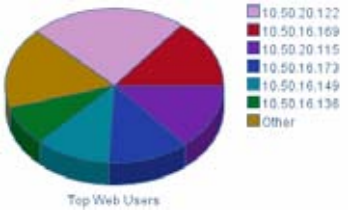
To edit the report settings, use the Search Bar at the top of the report. You can search other reports, set the start and end dates for a report to view, or click **More Options** to access other Report Display Settings. For a detailed description, see the “Searching for a Report” section on page 123.

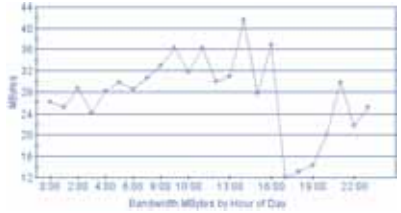
Selecting a Graphical Display

Some reports allow you to specify how many items to display in the report. Select **5**, **10**, **20**, **50**, **100**, or **All** from the **Number of Items** list. This allows you to limit the display to a the specified number in order to make the report easier to read.

Many reports offer different graphical displays for the data, such as a bar-graph or a pie chart. To select a graphical display, select **Chart and Table** under **Report Display Settings** and choose the display type from the **Chart Type** list. Your selection should display immediately in the report screen. For most reports you can choose **Area**, **Bar**, **Pie** or **Plot**.







Setting a Date or Date Range

Summary reports display only information for a single date. Over-time reports display information over a date range.

Selecting a Single Date

To select a single date for a report, click on the **Start** or **End** fields in the Search Bar to display the drop-down calendar. The End field is only configurable for Over Time reports. In the calendar, you can set the month by

clicking the single arrows (<, >), or the year by clicking the double arrows (<<, >>). To select the month or year from a drop-down list, click and hold the arrow button. Click **Search** to begin building the report.

Selecting a Date Range

To select a date range for an Over Time report, select a **Start Date** and **End Date** in the Search Bar, and then click **Search**. You can use the drop-down calendars by clicking in either field.

Additional Settings

Many reports have additional settings that you can select such as source and destination interfaces to report traffic through or how to display names and IP addresses. Make your selection from these lists and click **Search**.

Troubleshooting Reports

One of the most common error messages when a report does not display is “No Data”. There are several reasons why you might see this error, and SonicWALL ViewPoint 5.1 and higher displays the most likely reason and points you to the screen where you can make the necessary adjustments.

Some examples are shown in the following figures.

Figure 4 Appliance is Not Licensed for Reporting

This appliance is not licensed for ViewPoint Reporting
Click here to go to the General->Status page and look under "Not Licensed" section for steps to resolve the issue

Figure 5 Appliance is Down

Summary of Web Usage for July 9, 2008
No Data Available. The appliance is down.For more information Navigate to Policies->Status

Figure 6 Appliance in a Provisioned State

Web Usage Top Sites for July 9, 2008
No Data Available. The appliance is in provisioned state.For more information Navigate to Policies->Status

Figure 7 Configured for Status Only

Web Usage Top Sites for July 9, 2008
No Data Available. The appliance is configured to only send status messages.For more information Navigate to Policies->Management

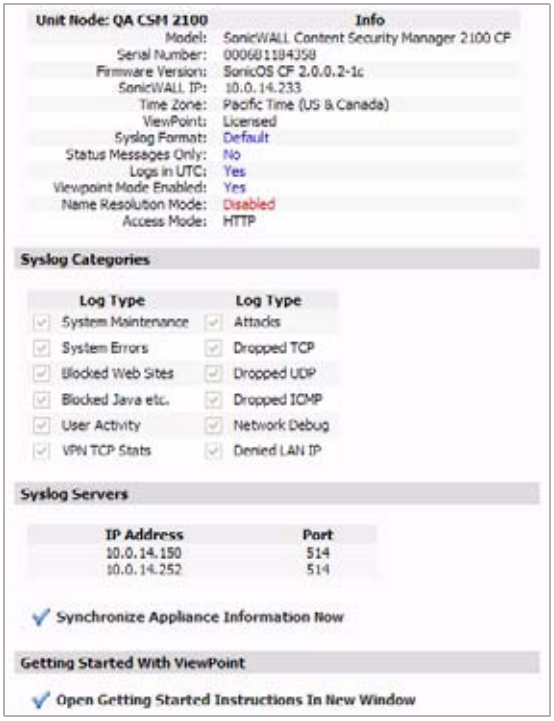
Viewing General Status Reports

The **General > Status** page contains information on the SonicWALL appliance or group of SonicWALL appliances.

To view the Status page, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **General** tree and click **Status**. The Status page displays.



4. The sections contain the following information:
   - Node information—Information on the firewall(s) is displayed at the global or unit level.
   - Syslog Categories—The types of syslog data selected to be collected for the selected appliance.
   - Syslog Servers—The IP address and Port number of the syslog servers configured to collect data from the selected appliance.
     - Synchronize Applicance Information with ViewPoint—Click the **Synchronize Applicance Information Now** link to refresh status data about the monitored appliances. This status information is normally updated every 24 hours.
   - Getting Started With ViewPoint—Click the **Open Getting Started Instructions In New Window** link to open the ViewPoint installation and initial configuration instructions in a separate window.

Viewing Dashboard Reports

Dashboard reports display an overview of bandwidth, uptime, intrusions and attacks, and alerts for managed SonicWALL UTM appliances. The Security Dashboard report provides data about worldwide security threats that can affect your network. The Dashboard also displays data about threats blocked by the SonicWALL security appliance.

Select from the following:

- "Viewing the Dashboard Summary Report" on page 159
- "Viewing the Security Dashboard Report" on page 162

Viewing the Dashboard Summary Report

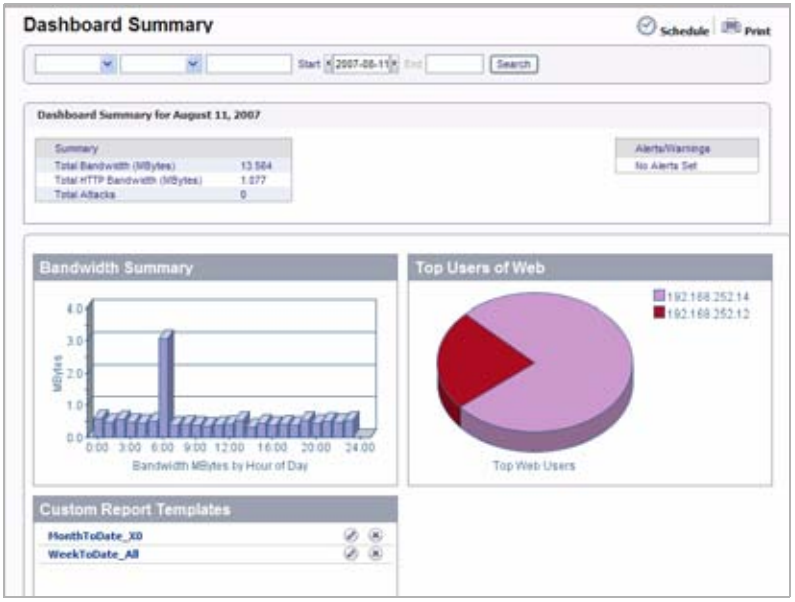
The Dashboard Summary report displays statistics, alerts, graphical summary reports, and a list of available custom report templates. Displayed statistics can include total bandwidth, total attacks and other measurable information. The alerts list is displayed when the configured threshold has been reached. A wide range of graphical reports are also available for display.

You can configure the Dashboard > Summary report contents in the UTM > Configuration > Dashboard page. For a description of the configuration procedure, see "Configuring Dashboard Summary Reports" section on page 142.

To view the Dashboard Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Dashboard** tree and click **Summary**.



4. The tables at the top of the page display the totals, using megabytes for the bandwidth totals.
5. The graphical display breaks down the information as follows:
   - **Bandwidth**—shown by group when viewed at global level. At the unit level, the bandwidth is shown per hour.
   - **HTTP Bandwidth**—at the unit level, this is shown as a pie chart with eight slices. The top seven Web users by IP address are each shown as a slice, with all other HTTP bandwidth combined in the eighth slice.
   - **Attacks Events**—at the global level, both attack events and virus attack attempts are shown per group. At unit level, these are shown per hour (not pictured).
   - **Custom Report Templates**—your “favorites” list of saved custom report templates. See “Using Custom Reports on UTM Appliances” on page 163.

     You can click the Edit icon next to the template on this page to edit the template in the Custom Report page and save it using the Save Template button. To delete the template, click the Delete icon.

Viewing Custom Reports on the Dashboard

SonicWALL ViewPoint provides access to your saved Custom Report templates on the Dashboard > Summary page for the appliance. The template must have been previously created and saved for the same appliance on the Custom Report > Internet Activity or Custom Report > Website Filtering page.

When you click on a saved template, the detailed report page is displayed in Full Mode with the same categories in the same order as in the template that you saved. In the report page, the Print, PDF, and Excel icons are available, along with the pagination controls. There is no link to Split Mode and no Save Template button since this template is already saved.

You can also configure or delete a saved template from the Dashboard > Summary page.

To access a custom report from the Dashboard:

1. Select a unit for which Log Viewer is enabled, and then navigate to **Dashboard > Summary**.
2. Locate the box labeled **Custom Report Templates**. All saved templates for this appliance are listed in the box.

3. Do one of the following:

- To generate a Custom Report, click a saved template in the **Custom Report Templates** box.
- To configure a saved template, click the Configure icon for that template, make the desired changes, and then click **OK**. For configuration instructions, see "Using Custom Reports on UTM Appliances" on page 163.
- To delete a saved template, click the Delete icon for that template and then click **OK** in the confirmation dialog box.

Viewing the Security Dashboard Report

The Security Dashboard report shows two types of reports:

- An Individual Appliance Report that displays a summary of attacks detected by the local SonicWALL security appliance.
- A Global Report that displays a summary of threat data received from all SonicWALL security appliances worldwide.

The Dashboard > Security Dashboard screen is available at the global level, but not at unit level for SonicWALL CSM Series appliances.

To view the Security Dashboard report, perform the following steps:

1. Click the **Reports** tab.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the **Dashboard** tree and click **Security Dashboard**. The Security Dashboard page displays.

Figure 8 Security Dashboard Page

4. At the top of the screen, select either the **Global** radio button or, for reporting at unit level, select the radio button that is labeled with the unit's MAC address. Select Global to display a summary of attacks caught by SonicWALL appliances worldwide. Select the unit's MAC address to see results only for attacks through this unit. At all levels, the categories charted include the following:
   - Viruses Blocked by SonicWALL Network
   - Intrusions Prevented by SonicWALL Network
   - Spyware Blocked
   - Multimedia (IM/P2P) Detected/Blocked

For each of these, the report includes the results over time for the top ten.

5. Optionally select the period of time for the report from the drop-down box at the top right of each graphical display. At the unit level, you can select only the **Last 21 days**. At the global or group level, you can select from:
   - Last 12 Hours
   - Last 14 Days
   - Last 21 Days
   - Last 6 Months

Using Custom Reports on UTM Appliances

Custom Reports are available at the unit level for appliances visible on the UTM tab. Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see "Viewing the Log" on page 290.

When configuring a Custom Report on the Internet Activity or Website Filtering page, the Template Section acts as a query builder. You select the criteria for the report that you want, and SonicWALL ViewPoint uses your input to query the raw syslog database for the information, and then outputs the report. The Template Section consists of two parts: the Date/Time section and the Report Layout section.

After building your query in the Template Section and clicking the **Generate Report** button, the report is displayed in the Report Section. The Report Section is displayed in the lower half of the page, under the Template Section; this layout is called Split Mode. You can easily toggle between Split Mode and Full Mode. Full Mode can be used to display only the Template Section or only the Report Section in a full page view.

The Report Section displays the report and provides controls for pagination, printing, and exporting the report in PDF or CSV format. You can also click the **Save Template** button in this section if you want to save the settings for this report as a template for reuse later.

See the following sections for detailed information:

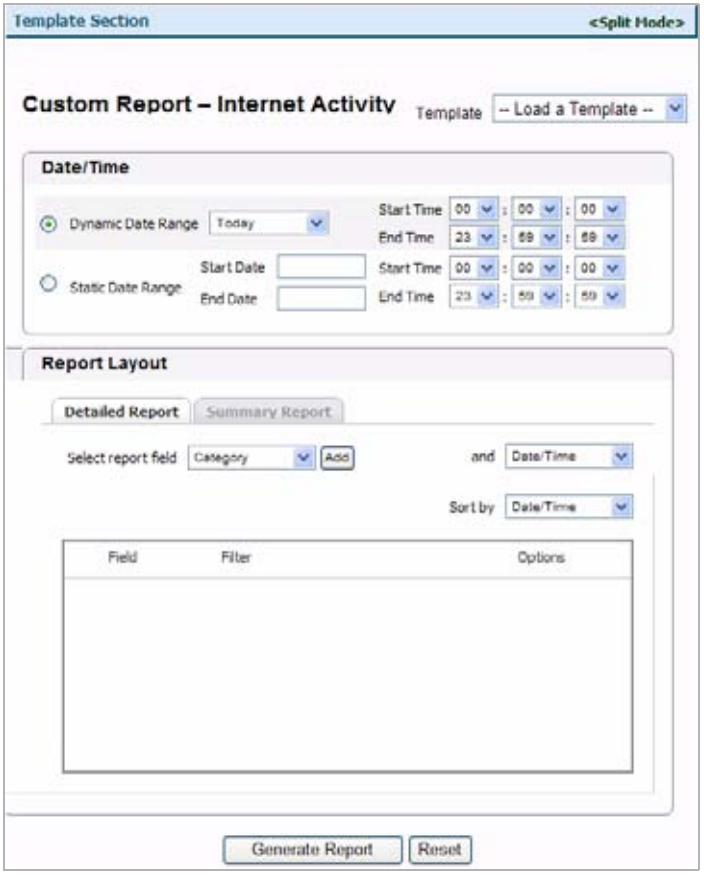
- "Toggling Between Split Mode and Full Mode" on page 164
- "Configuring the Date and Time for Custom Reports" on page 166
- "Configuring the Report Layout and Generating the Report" on page 168
- "Generating the Custom Report" on page 176
- "Viewing a Custom Report" on page 177

- "Printing a Page or Exporting the Report as a PDF or CSV File" on page 179
- "Saving the Report Template" on page 180

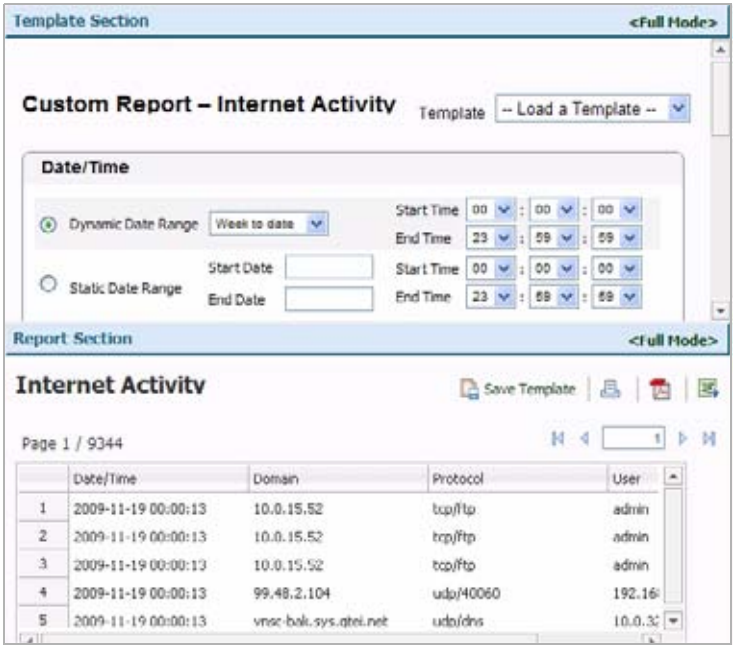
Toggling Between Split Mode and Full Mode

The Custom Report page contains two main sections, the Template Section and Report Section, which can be displayed together or independently depending on the mode.

When the Custom Report page is initially displayed for a selected appliance, the Template Section is displayed in Full Mode. Split Mode is available, but the Report Section displays no data until a report has been generated. The Custom Report > Internet Activity page with the Template Section displayed in Full Mode is shown below.



After generating a report, the page automatically changes to Split Mode and displays the report settings in the Template Section in the top half of the page and the report results in the Report Section in the lower portion. The Template Section and Report Section displayed in Split Mode is shown below.



At any time, you can change to Full Mode if you want to display either the Template Section or the Report Section individually. From Full Mode, you can easily change back to Split Mode.

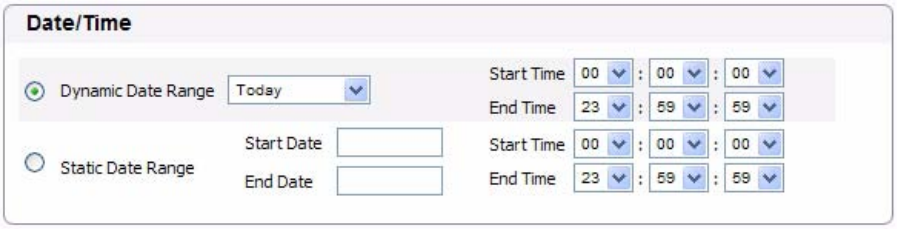
To toggle between Split Mode and Full Mode:

1. Select a unit for which Log Viewer is enabled, and then navigate to the **Custom Report** page.
2. On a page that is currently displayed in Full Mode, to change the view to Split Mode click the **<Split Mode>** button at the right side of the section heading.
3. On a page that is currently displayed in Split Mode, do one of the following to change to a Full Mode display of either the Template Section or the Report Section:
   - Click the **<Full Mode>** button to the right of the Template Section heading.
   - Click the **<Full Mode>** button to the right of the Report Section heading.

Configuring the Date and Time for Custom Reports

At the top of the Template Section of the Custom Report page, the Date/Time region provides a way to designate the time period to use when generating the report. You can select either a Dynamic Date Range or a Static Date Range.

Both the Dynamic Date Range and the Static Date Range provide Start Time and End Time settings. By using the Start Time and End Time fields, you can specify the exact hour, minute, and second for both the beginning and the end of the period for the report. When a start and end time is specified for a date range containing multiple days, the start/end times are applied to each day of the period when analyzing data for the report. The default is to include data for the full 24 hours in each day of the date range.



Dynamic Date Range

The **Dynamic Date Range** selection allows you to select from four date ranges and to specify the exact starting and ending times on the days in the selected date range for the log data to be used for the report.

For the **Dynamic Date Range**, you can select from the following four date choices:

- **Today** – Uses log data from the current date, beginning just after midnight
- **Yesterday** – Uses log data from just after midnight of the previous day, up to and including the most recent log message from the current date
- **Week to Date** – Uses log data from the current date, plus the seven preceding days
- **Month to Date** – Uses log data from the same date as the current date in the previous month, up to and including the most recent log message from the current date

When generating a report with a template containing a dynamic date range setting, the dates used when referencing the log data are relative to the current date. Thus, two reports generated from the same template on different days will provide different results.

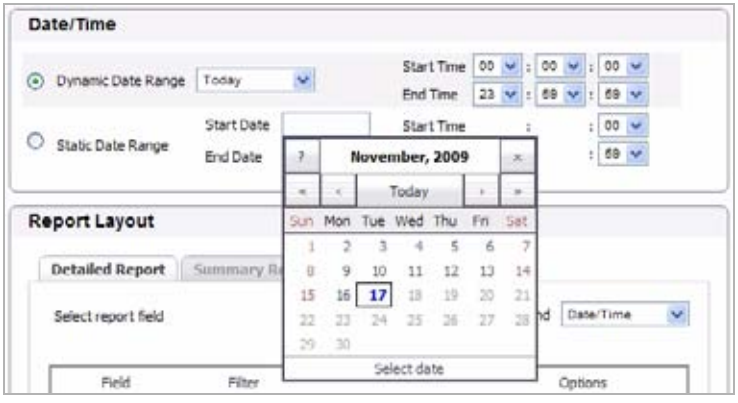
To select a Dynamic Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Dynamic Date Range** radio button.
3. In the drop-down list, select **Today**, **Yesterday**, **Week to Date**, or **Month to Date**.
4. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Dynamic Date Range row. These settings specify the earliest data to be included in the report, for each day of the date range.
5. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data to be included in the report, for each day of the date range.
6. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Static Date Range

The **Static Date Range** selection allows you to specify the exact dates, starting, and ending times on the days in the selected date range for the log data to be used for the report. You can specify a single date or a date range, and indicate the exact hour, minute, and second for both the beginning and the end of the daily period for the report.

A popup calendar makes it easy to select the Start Date and End Date for the date range.



To specify a Static Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Static Date Range** radio button.
3. Click the **Start Date** field to access the pop-up calendar.
4. Use the navigation arrows near the top of the calendar to change the year or month. Click the **<<** button to move to the previous year, or hold the button to select from a list of years. Click the **>>** button to move to the next year, or hold the button to select from a list of years. Similarly, click the **<** or **>** to move back or ahead by one month, or hold the button to select from a list of months.
5. Click the desired start date in the calendar. This adds the date to the **Start Date** field and closes the calendar.
6. Click the **End Date** field to access the pop-up calendar.
7. Use the navigation arrows near the top of the calendar to change the year or month.
8. Click the desired end date in the calendar. This adds the date to the **End Date** field and closes the calendar.
9. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Static Date Range row. These settings specify the earliest data for each day in the date range to be included in the report.
10. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data for each day in the date range to be included in the report.
11. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Configuring the Report Layout and Generating the Report

Located in the Template Section of the Custom Report page below the Date/Time region, the Report Layout region provides a way to specify the type of data to include, and the format of the report. The Report Layout region has a Detailed Report tab and a Summary Report tab. The report appearance and the way information is organized is quite different between a Detailed Report and a Summary Report.

The Detailed Report tab contains a list of data categories that you can add as report fields, and allows you to specify query values for each. The categories you select will appear as column headings in the report.

The Summary Report tab allows you to structure a report showing the top elements of Internet Activity or Website Filtering. You can select the number of top elements, what to base the comparisons on, and the two data categories to evaluate when determining the top elements. The generated report provides graphical output that you can click to drill down for detailed information.

For more information about each of these Report Layout tabs, see the following sections:

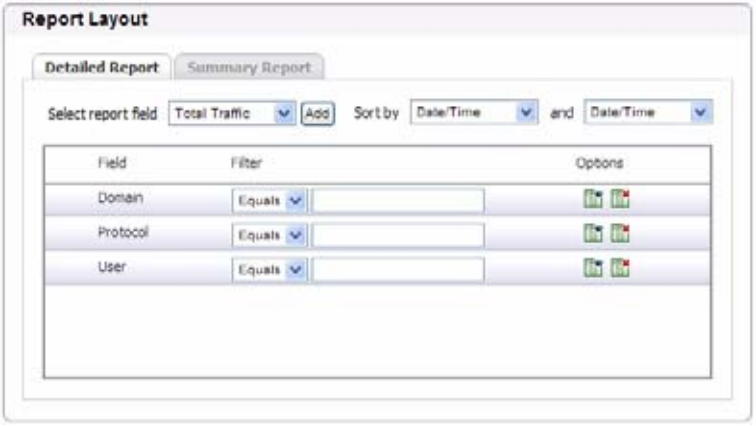
- "Detailed Reports" on page 169
- "Summary Reports" on page 173

For information about the Filter operators, see the following section:

- "Filter Operators" on page 175

Detailed Reports

The Detailed Report tab is the default view in the Report Layout region.



For a UTM Internet Activity report, the **Select Report Field** drop-down list contains eight data categories that you can add as column headings in the report. The categories are:

- **Full URL** – Adds a column containing the full URL of each Web site visited
- **Category** – Adds a column containing the category of each site visited, such as Gambling or Adult/Mature Content

- **Domain** – Adds a column containing the domain name of each site visited
- **Protocol** – Adds a column containing the protocol used by the traffic
- **Received Traffic**– Adds a column containing the number of bytes received from the visited site
- **Transmitted Traffic** – Adds a column containing the number of bytes transmitted to the site
- **Total Traffic** – Adds a column containing the total number of bytes received and transmitted
- **User** – Adds a column containing the user ID

For a UTM Website Filtering report, the **Select report field** drop-down list contains four data categories that you can add as column headings in the report. The categories are:

- **Full URL** – Adds a column containing the full URL of each logged Web site
- **Category** – Adds a column containing the category of each logged site, such as Gambling or Adult/Mature Content
- **Domain** – Adds a column containing the domain name of each logged Web site
- **User** – Adds a column containing the user ID

To include a field in the report, select a choice from the list and then click **Add**. When you click **Add**, a row is populated in the table below, which has three column headings: Field, Filter, and Options.

Note When you place your mouse cursor over the row, under the Field heading, the cursor changes to a “move” cursor. You can drag and drop the rows to rearrange the column ordering in the final report.

In the Filter column, two fields are displayed: an operator field and an input field. The operator field is a drop-down list containing the operator choices for the selected report field. See “Filter Operators” on page 175 for a description of each operator. The input field can be a drop-down list or a standard input field, depending on the selected report field.

The operators and input fields are defined in Table 5 for each report field.

Table 5 Operators and Input Fields for Each Data Type

Data Type	Operators	Input Field
Category	Equals	The input field is a drop-down list containing an alphabetized list of all the content filtering categories, such as Adult/Mature Content, Gambling, Military, etc. Leave the default of All in the input field if you choose not to filter by a certain category.
Destination IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain destination IP address.
Domain	Equals Start with End with Contains	The input field is a standard input field where you can type in the domain to match, such as sonicwall.com. Leave the input field blank if you choose not to filter by a certain domain.
Full URL	Equals Start with End with Contains	The input field is a standard input field where you can type in the URL to match, such as: `http://www.funnyyoutubevideo.com/funniest.html` Leave the input field blank if you choose not to filter by a certain URL.
Protocol	Equals Start with End with Contains	The input field is a standard input field where you can type in the protocol to match, such as FTP. Leave the input field blank if you choose not to filter by a certain protocol.
Received Traffic	= > >= < <= !=	The input field is a standard input field where you can type in the number of bytes to match or compare to. Leave the input field blank if you choose not to filter by a certain amount of traffic.
Source IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain source IP address.
Total Traffic	= > >= < <= !=	The input field is a standard input field where you can type in the number of bytes to match or compare to. Leave the input field blank if you choose not to filter by a certain amount of traffic.

Data Type	Operators	Input Field
Transmitted Traffic	= > >= < <= !=	The input field is a standard input field where you can type in the number of bytes to match or compare to. Leave the input field blank if you choose not to filter by a certain amount of traffic.
User	Equals Start with End with Contains	The input field is a standard input field where you can type in the user ID to match. Leave the input field blank if you choose not to filter by a certain user.

In the Options column, two icons are displayed: an Eye and an X . You can click the Eye to toggle whether the report field on that row will be displayed in the final report. This allows you to filter the report results based on the selected report field and related filter value, but not display the field as a column. When you click on the Eye icon within a row, the eye closes to show that this field will not be displayed in the final report. The filter value will still be used to filter results from the raw syslog database to apply towards the report.

For example, you might specify the following Field/Operator/Filter Value: **Protocol/=/http**. It would make sense to click the Eye icon to disable the Protocol field from being shown in the report, since it would always just be “http” and would not add any interesting information to the final report. Contrast this with simply specifying the Protocol field and leaving the Filter Value blank, in which case you would want to enable the Eye so that this column would appear in the report showing a variety of protocols such as udp/dns, tcp/http, udp/ntp, or numbered protocols such as udp/389 (the LDAP protocol) or tcp/445 (MS Server Message Block (SMB) file sharing).

Clicking the X icon under Options deletes the selected report field from the table, so it will not be used to generate the report results nor will it be displayed in the report. Use the X icon instead of the Eye when you do not choose to filter the report results based on the field.

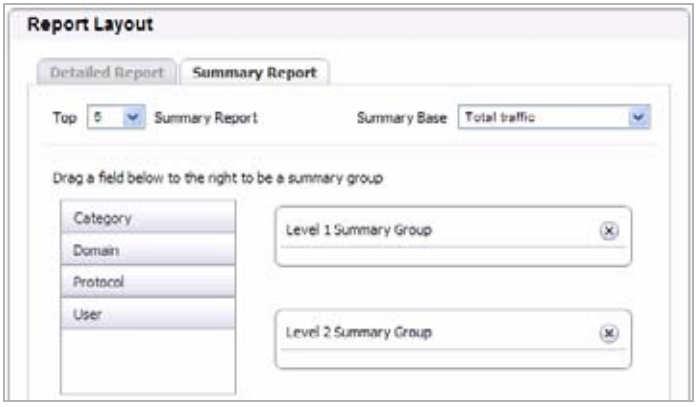
The Detailed Report tab also contains the Sort By drop-down list. The list contains the Date/Time option and any other report fields that you have selected from the eight data types. The choice you select will be used to order the results in the report from the first page to the last. The selection in the left drop-down list is used for the first sorting, then the selection in the right drop-down list is used to sort and group the entries within each group resulting from the the first sorting.

To configure a detailed report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Detailed Report** tab.
3. In the **Select report field** drop-down list, select a data type to include in the report, and then click **Add**. A row for this field is populated in the table below. Repeat this step to add other fields.
4. Optionally select an operator from the drop-down list under **Filter** in a table row, and type in or select an input value to be matched when the database is queried. Repeat this step for other rows to add filter values for those fields.
5. To prevent a field from appearing in the final report, click the **Eye** icon in that row so that the eye appears closed. To allow the field to be displayed in the report, click the closed **Eye** icon to return it to normal appearance.
6. To delete a field from the table, click the **X** icon in that row.
7. To sort the report pages by a different field than the default of Date/Time, select the desired field from the **Sort by** drop-down list.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region and the Report Layout region back to default settings.

Summary Reports

The Summary Report tab is available in the Report Layout region of the Template Section.



The Top drop-down list provides selections for the number of entries to display in the report. For example, if the User field is selected below as a Summary Group, and 5 is selected in the Top drop-down list, the report will provide entries for the top five users. For all Custom Reports, available numbers in the Top drop-down list are 5, 10, 20, 50, and 100.

The Summary Base drop-down list offers a selection of traffic types that will be used to determine the top usage for the selected field. The Summary Base choices vary as follows depending on the type of Custom Report:

- For a UTM Internet Activity report, the Summary Base choices are Total traffic, Received traffic, or Transmitted traffic.
- For a UTM Website Filtering report, the only Summary Base choice is Filtered Items.

Below the Top and Summary Base fields, you can create one or two Summary Groups from the choices listed on the left side. The Summary Groups choices vary as follows depending on the type of Custom Report:

- For a UTM Internet Activity report, the choices are Total traffic, Received traffic, or Transmitted traffic.
- For a UTM Website Filtering report, the choices are Category, Domain, or User.

To select a field for a Summary Group, simply drag and drop the desired field from the list to either the Level 1 Summary Group or Level 2 Summary Group boxes. When the field name is dragged to one of these, the operator drop-down list and filter input value field are displayed, allowing you to specify values to match when the data is searched. See "Filter Operators" on page 175 for a description of each operator.

Either the Level 1 Summary Group field or the Level 2 Summary Group field can be used alone; the resulting report will look the same in both cases.

When both the Level 1 and Level 2 Summary Group fields are populated, the report will display the top entries for the Level 2 field for each of the top entries for the Level 1 field. For example, if User is dragged to the Level 1 Summary Group and Domain is dragged to the Level 2 Summary Group, and 5 is selected in the Top drop-down list, the generated report will display the top five domains visited by each of the top five users.

To configure a summary report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Summary Report** tab.

3. In the **Top** drop-down list, select the number of entries to be displayed in the report.
4. In the **Summary Base** drop-down list, select one of the choices to use when determining which are the top elements in the selected field.
5. To specify the field for the **Level 1 Summary Group**, click and drag the desired field from the list on the left to the **Level 1 Summary Group** field, and then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.

6. To specify the field for the **Level 2 Summary Group**, click and drag the desired field from the list on the left to the **Level 2 Summary Group** field, then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.
7. To specify a filter operator and filter value for a Summary Group, select the operator from the drop-down list next to the field and type a filter value into the input field to the right of the operator.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region as well as the Report Layout region back to default settings.

Filter Operators

When configuring the Report Layout on either the Detailed Report tab or the Summary Report tab, you can specify filter values to be matched in the database during report generation. Depending on the selected field type, text string or numeric, several filter operators are available. The filter operators are used with a filter input value to determine which data should be included in the report.

The operators are defined as shown in Table 6.

Table 6 Filter Operators

Operator	Definition
Equals	Only data that exactly matches the filter input text will be included in the report
Start with	Data that begins with the input text will be included in the report

Operator	Definition
End with	Data that ends with the input text will be included in the report
Contains	Data that contains the input text will be included in the report
=	Only data that exactly matches the filter input numerical value will be included in the report
>	Data values that are greater than the input numerical value will be included in the report
>=	Data values that are greater than or equal to the input numerical value will be included in the report
<=	Data values that are less than or equal to the input numerical value will be included in the report
<	Data values that are less than the input numerical value will be included in the report
!=	Data values that are not equal to the input numerical value will be included in the report

Generating the Custom Report

The Generate Report button at the bottom of the Template Section is used to create the report. Before clicking Generate Report, use the Template Section to specify the time period for the report and the contents and layout of the report.

Note Custom Reports are available at the unit level and Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see “Viewing the Log” on page 290.

To generate a custom report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report you want.
2. In the **Date/Time** region of the Template Section, specify the time period that the report will cover. For detailed information and instructions, see “Configuring the Date and Time for Custom Reports” on page 166.

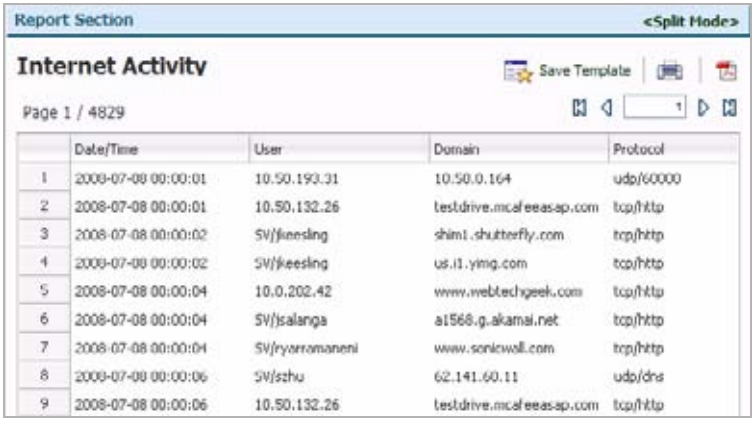
3. In the **Report Layout** region of the Template Section, specify the contents and appearance of the report. For detailed information and instructions, see "Configuring the Report Layout and Generating the Report" on page 168.
4. Click **Generate Report** to create the report using the specified configuration.

Viewing a Custom Report

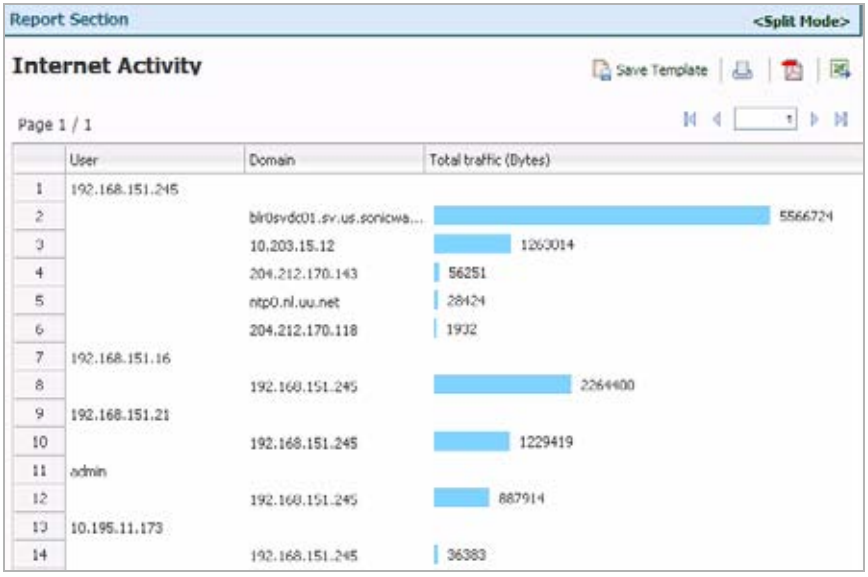
After you click Generate Report, the Report Section is displayed in Split Mode in the lower half of the main window, even if you previously were in Full Mode for the Template Section.

Pagination controls are displayed at the upper right of the report, just below the Save Template button and the printer, PDF, and Excel icons. Navigation buttons are provided to take you to the first page, next page, previous page, and last page, or you can specify an exact page number in the field.

In a Detailed Report, shown below, the selected report fields are displayed as column headings. You can click on any column heading to sort that page by the values in the column that you click. Click again to toggle between ascending and descending order on that page. When you navigate away from that page and then come back using the pagination controls, the page reverts to the original sorting order as specified in the **Sort by** field of the Template Section before generating the report.

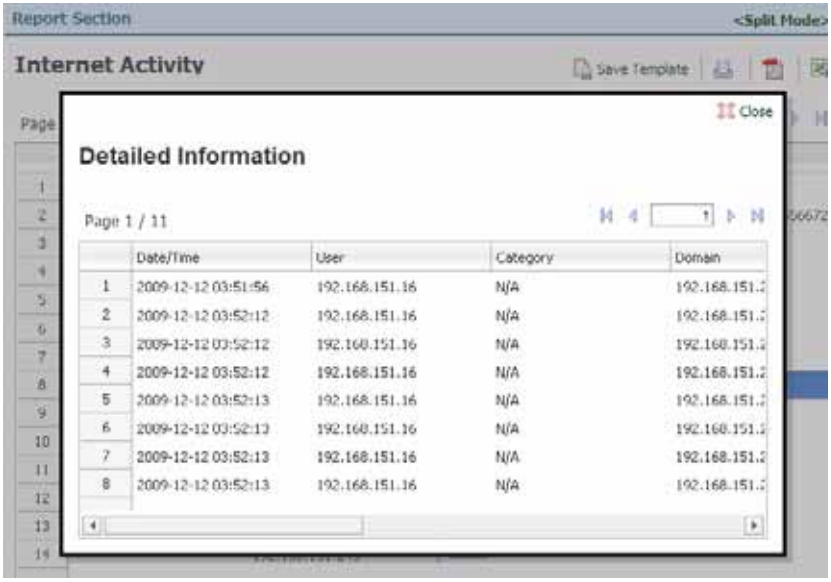


In a Summary Report, the Report Section displays the traffic volume as horizontal bar charts. This lets you see the information at a glance, such as who consumed the most bandwidth and which domains they visited the most.



You can click on a bar in the chart to pop up detailed information, just like the detailed report with all of the columns for all fields. The report lists details about this Summary Group field only. For example, in the Internet Activity report, if the Summary Group contains the User field and you click on a bar for one of the top users, the report displays the date and time of all Internet activity for the user, and includes data for every field available for detailed reports. A scroll bar is provided along the bottom of the Detailed Information window to allow viewing of all eight fields plus the date and time column.

The Detailed Information window is shown below.



Printing a Page or Exporting the Report as a PDF or CSV File

To print the current page of the report, click the printer icon at the top of the Report Section. Your normal print dialog box pops up. This prints only the page that is currently displayed.

To export the entire report in PDF format, click the PDF icon at the top of the Report Section. A PDF file is generated showing the report results in table format.

To export the entire report in Microsoft Excel Comma Separated Value (CSV) format, click the Excel icon at the top of the Report Section. A CSV file is generated showing the report results in spreadsheet format.

The PDF can contain a maximum of 10,000 records. If your report contains more than 10,000 records, you can use the Static Date Range fields to adjust the dates and regenerate the report to shorten its length. You can save the PDF or CSV file using any filename and location.

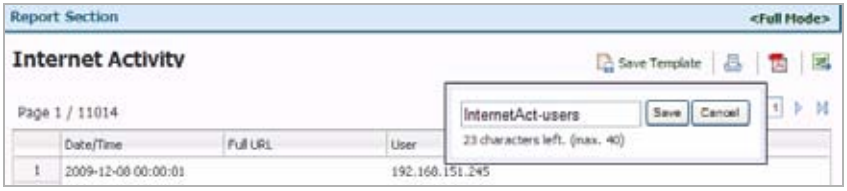
Saving the Report Template

After generating the report, you can save the settings for this report as a template for reuse. You can select the saved template from the Template Section or from the Dashboard > Summary page at a later time, and use it to generate a report using the same settings. For information about using the template on the Dashboard > Summary page, see “Troubleshooting Reports” on page 156.

The template is saved for the currently selected appliance and for the specific user. The saved template will not be available for other appliances or for other users.

To save the report template:

1. In the Report Section in the upper right corner, click the **Save Template** button.



2. In the popup dialog box, type in a descriptive name for the template, up to 40 characters. The number of remaining characters allowed in the name is displayed below the input field and changes as you type.
3. Click **Save**. If you are in a Full Mode display of the Report Section, you can verify that the template has been saved by changing back to Split Mode and viewing the contents of the **Template** drop-down list.

SonicWALL ViewPoint provides access to your saved Custom Report templates on the Dashboard > Summary page for the appliance. See “Viewing Custom Reports on the Dashboard” on page 161.

Viewing Bandwidth Reports

Bandwidth reports display the amount of data transferred through one or more selected SonicWALL appliances. These reports include the cost of consumed network bandwidth per 100 megabytes transferred through the selected appliances.

Bandwidth reports are an ideal starting point for viewing overall bandwidth usage. You can view bandwidth usage view by hour, day, or over a period of days. Additionally, you can view the top users of bandwidth.

From this information, you can determine network strategies. For example, if you need more bandwidth, you might need to upgrade network equipment, or you might simply need to curtail the bandwidth usage of a few employees.

Note All reports appear in the appliance's time zone.

Select from the following:

- "Viewing the Bandwidth Summary Report" on page 181
- "Viewing the Top Users of Bandwidth" on page 183
- "Viewing Bandwidth Usage Over Time" on page 185
- "Viewing the Top Users of Bandwidth Over Time" on page 187

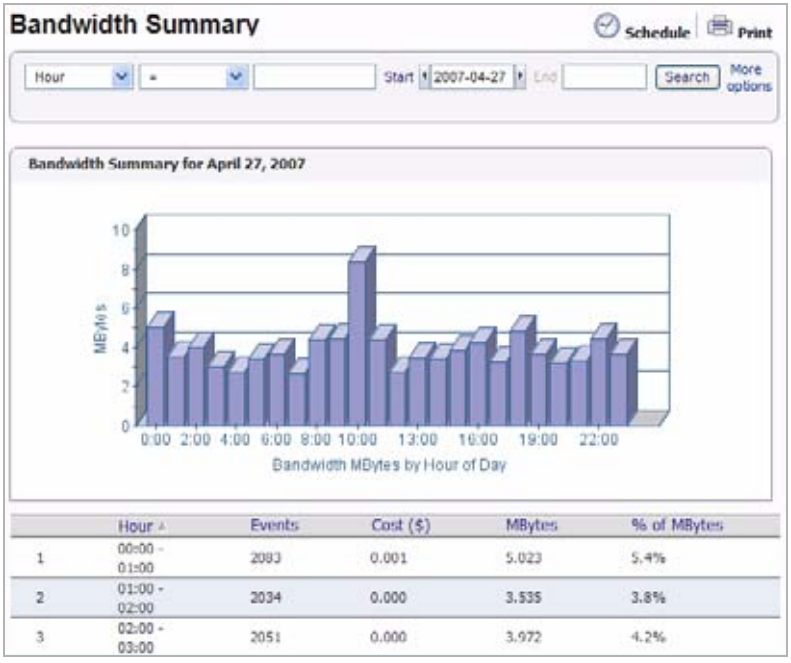
Viewing the Bandwidth Summary Report

The Bandwidth Summary report contains information on the amount of traffic handled by a SonicWALL appliance during each hour of the specified day, or at the global level, for all SonicWALL appliances for the day.

To view the Bandwidth Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Bandwidth** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the amount of bandwidth transferred during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or “hits.”
   - **Cost ($)**—amount of the expense per 100 megabytes. You can configure this in the **Cost Per Mega Byte Bandwidth Use** field in the Console > Reports > Summarizer screen.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date of the report and other settings, click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:

- **Display Type**: **Chart and Table**, or **Table Only**
- **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
- Select the **Source** and **Destination** interfaces to view
- If you want to track bandwidth usage in both directions, select the **Bi-directional** check box.

See "Managing Report Settings" on page 154.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note These settings will stay in effect for all summary reports during your active login session.

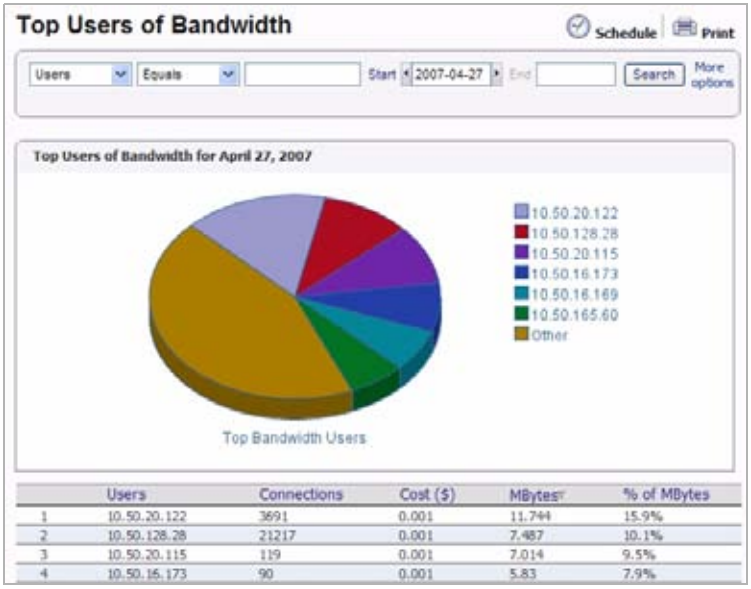
Viewing the Top Users of Bandwidth

The Top Users report displays the users who used the most bandwidth on the specified date and the correlating expense.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Bandwidth** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of bandwidth transferred by each user.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or “hits.”
   - **Cost ($)**—amount of the expense per 100 megabytes. You can configure this in the **Cost Per Mega Byte Bandwidth Use** field in the Console > Reports > Summarizer screen.
   - **MBytes**—number of megabytes.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. By default, the ViewPoint Reporting Module shows yesterday’s report, a pie chart, and the ten top users. To change the date of the report and other settings, click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. To display a limited number of users, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note These settings will stay in effect for all similar reports during your active login session.

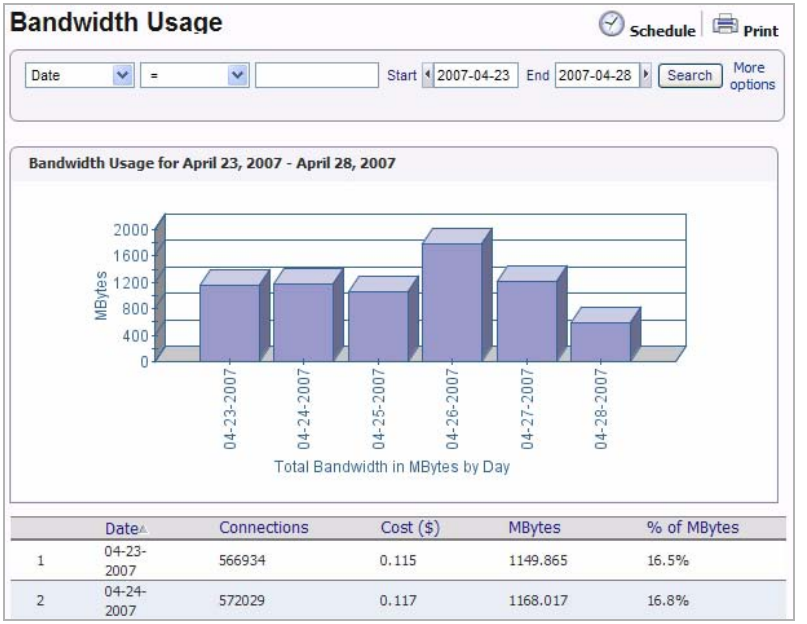
Viewing Bandwidth Usage Over Time

The Bandwidth Over Time report displays the daily amount of traffic and the total daily expense for consumed network bandwidth handled by a SonicWALL appliance or a group of SonicWALL appliances for the specified time period.

To view the Bandwidth Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Bandwidth** tree and click **Over Time**. The Over Time page displays.



	Date	Connections	Cost ($)	MBytes	% of MBytes
1	04-23-2007	566934	0.115	1149.865	16.5%
2	04-24-2007	572029	0.117	1168.017	16.8%

4. The bar graph displays the amount of bandwidth transferred during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of hits.
   - **Cost ($)**—amount of the expense per 100 megabytes. You can configure this in the **Cost Per Mega Byte Bandwidth Use** field in the Console > Reports > Summarizer screen.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% of MBytes** field will display 25%.
6. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** fields to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**

– **Chart Type**: **Area**, **Bar** or **Plot** chart

See “Managing Report Settings” on page 154.

8. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date range.

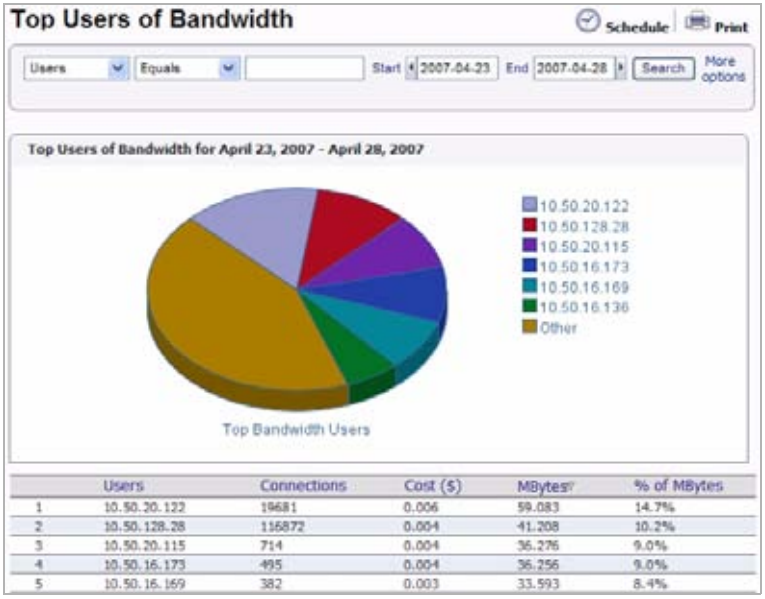
Note These settings will stay in effect for all similar reports during your active login session.

Viewing the Top Users of Bandwidth Over Time

The Top Users Over Time report displays the users who used the most bandwidth and accumulated the highest cost during the specified date range. This report is available at the unit level.

To view the Top Users Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Bandwidth** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the percentage of bandwidth transferred by each user.

5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or “hits.”
   - **Cost**—total amount of the expense per 100 megabytes.
   - **MBytes**—number of megabytes.
   - **% of MBytes—**percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during this period and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report and other settings, click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. To display a limited group of users, enter the user IDs in the **Search Bar** fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

9. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected users and date range.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Services Reports

Service reports provide information on the amount of data transmitted through the selected SonicWALL appliance by each service.

Service reports are useful for revealing inappropriate usage of bandwidth and can help determine network policies. For example, if there is a large spike of bandwidth usage, you can determine whether this is caused by regular Web access, someone using FTP to transfer large files, an attempted Denial of Service (DoS) attack, or another service.

Note All reports appear in the appliance's time zone.

The procedures for viewing the Services Reports are described in the following section:

- "Viewing the Services Summary Report" on page 189

Note You cannot view services reports from the global view.

Viewing the Services Summary Report

The Services Summary report displays the amount of traffic handled by each service during each hour of the specified day.

To view the Services Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Services** tree and click **Summary**. The Summary page displays.

4. The bar graph displays the amount of bandwidth used by each service during each hour of the day.
5. The table contains the following information:
   - **Protocol**—the service.
   - **Events**—number of events or "hits."
   - **MBytes**—Number of Megabytes.
   - **% of MBytes**—percentage of megabytes transferred by this service on the selected day, compared to all other services. For example, if 10,000 megabytes of data was transferred during the day and 5,000 of the megabytes were transferred, the **% of MBytes** field will display 50%.
6. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See "Managing Report Settings" on page 154.

8. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage Reports

Web usage reports provide information on the amount of Web usage that occurs through the selected SonicWALL appliance(s).

Web usage reports can be used to view Web bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of Web bandwidth and view the most visited sites. Exclusion settings for Web sites and Web users are available on the Console > User Settings > Reports page. Web Usage reports will not contain references to the Web sites or users specified on this page. For more information, see the “Configuring Reports Settings” section on page 53.

For the Summary and Over Time reports, and for all reports involving Users, the browse time is also provided in one column of the table. The browse time is the amount of time consumed browsing the Internet through one or more selected SonicWALL appliances. The browse time is not displayed in reports for Category or Sites.

Note All reports appear in the appliance’s time zone.

Select from the following:

- “Viewing the Web Usage Summary Report” on page 192
- “Viewing the Top Web Sites” on page 194
- “Viewing the Top Users of Web Bandwidth” on page 195
- “Viewing Web Usage by User” on page 197
- “Viewing Web Usage By Site” on page 199
- “Viewing Web Usage By Category” on page 200
- “Viewing Web Usage Over Time” on page 202
- “Viewing Top Sites Over Time” on page 203
- “Viewing Top Users Over Time” on page 205
- “Viewing Web Usage By User Over Time” on page 207

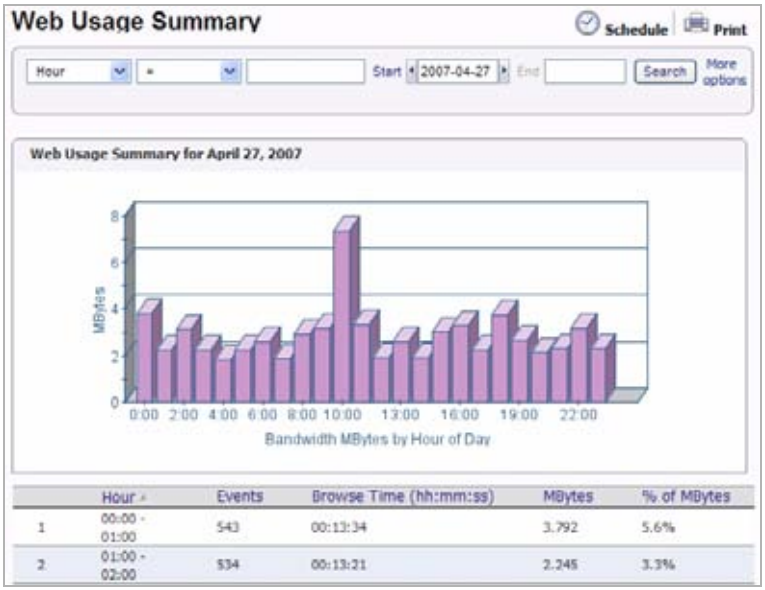
- “Viewing Web Usage By Category Over Time” on page 208

Viewing the Web Usage Summary Report

The Web Usage Summary report contains information on the amount of HTTP bandwidth handled by a SonicWALL appliance or all SonicWALL appliances during each hour of the specified day. The report includes information on the amount of time spend browsing the Internet behind a SonicWALL appliance or all SonicWALL appliances.

To view the Web Usage Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the amount of HTTP bandwidth transferred during each hour of the day.

5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or “hits.”
   - **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.

     Browse Time is calculated as follows:

     (Number Of Pages / Noise Reduction Factor) * Average Browse Time Per Page

     "Number Of Pages" is the number of hits (responses by the Web site to build the page) when a User accesses a Web page (www.sonicwall.com).

     "Noise Reduction Factor" is the average noise we want to exclude per page (like eliminating pop-up links, images, and more). The factory default is 40.

     "Average Browse Time Per Page" is the time allocated to read a page.

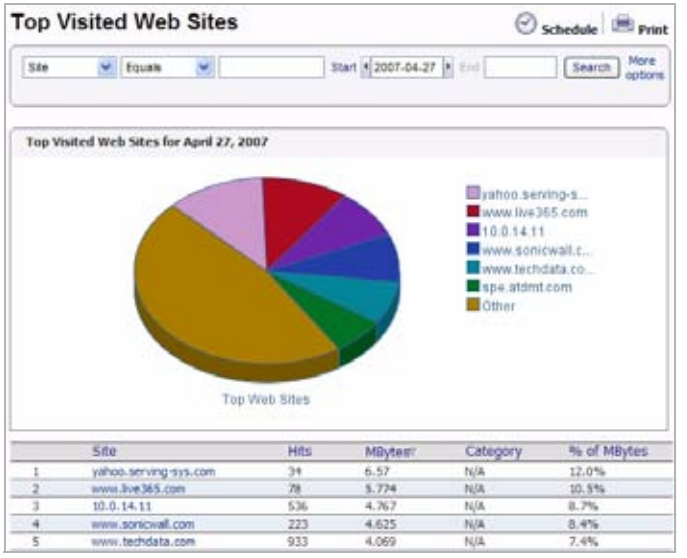
     Noise Reduction Factor and Average Browse Time Per page are configurable in the database directly, but are not exposed in ViewPoint management interface.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of HTTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
6. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Top Web Sites

The Top Sites report displays the Web sites that used the most HTTP bandwidth on the specified date. To view the Top Sites report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **Top Sites**. The Top Sites page displays.



	Site	Hits	MBytes	Category	% of MBytes
1	yahoo.serving-sys.com	34	6.57	N/A	12.0%
2	www.live365.com	78	5.774	N/A	10.5%
3	10.0.14.11	536	4.767	N/A	8.7%
4	www.sonicwall.com	223	4.625	N/A	8.4%
5	www.techdata.com	933	4.069	N/A	7.4%

4. The pie chart displays the percentage of bandwidth used to access the top sites.
5. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **Category**—the Web site category.
   - **% of MBytes**—percentage of megabytes transferred between this site, compared to all other HTTP traffic. For example, if 10,000 megabytes of data was transferred during the day and 5,000 megabytes was transferred between the appliance and Ebay, the **% of MBytes** field will display 50% and you have a problem.

6. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Sites**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date.

Note These settings will stay in effect for all similar reports during your active login session.

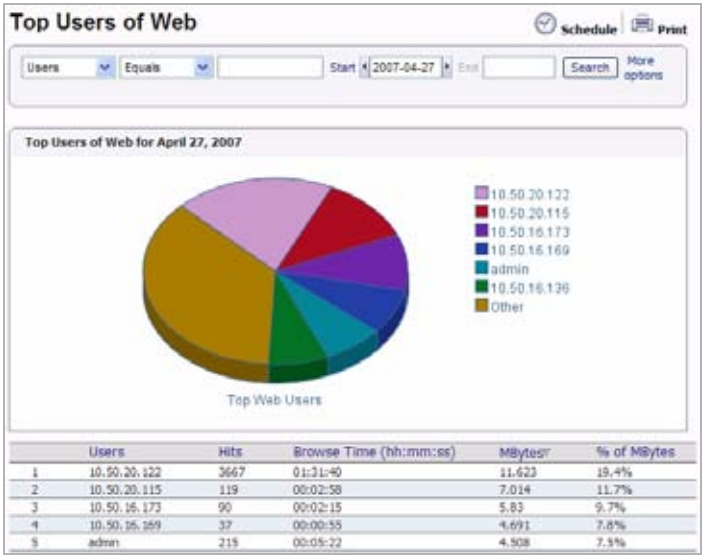
Viewing the Top Users of Web Bandwidth

The Top Users report displays the users who used the most HTTP bandwidth and the amount of time they spent browsing the Internet on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Usage** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of bandwidth transferred by each of the top users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Hits**—number of hits.
   - **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. To display a limited group of users, enter the user IDs in the **Search Bar** fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage by User

The By User report displays a list of all users, their top sites, the number of hits to each site, the time spent browsing, and the amount of data transferred.

To view the By User report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Usage** tree and click **By User**. The By User page displays.

4. The table contains the following information:
   - **User**—the IP address of the user.
   - **Hits**—the number of hits to each Web site visited by the user.
   - **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.
   - **MBytes**—the number of megabytes transferred.
5. You can navigate directly from the **Web Usage > By User** page to a **Web Usage > By Site** page detailing the information of the site the user has been browsing. Click the **Plus** sign to the left of the **User** name or IP address to show details, and then hover the mouse over a site. A sticky tooltip will display with a link to the corresponding site's report page.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report and other settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Number of Users**
   - **Number of Sites per User**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. To display a limited group of users, enter the user IDs in the **Search Bar** fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage By Site

The By Site report displays a list of all sites, the users that accessed the sites, the number of hits to each site, and the amount of data transferred.

To view the By Site report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **By Site**. The By Site page displays.

4. The table contains the following information:
   - **Site**—the URL of the site.
   - **Hits**—the number of hits to the Web site, by user.
   - **MBytes**—the number of megabytes transferred, by the user.
   - **Category**—the category of the site.

5. You can navigate directly from the **Web Usage > By Site** page to a **Web Usage > By User** page detailing the information of the users who have been browsing the site. Click the **Plus** sign to the left of the **Site** to show details, and then hover the mouse over a user. A sticky tooltip will display with a link to the corresponding user report page.
6. The ViewPoint Reporting Module shows yesterday's report and all Web sites. To change the date of the report or Web sites displayed, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Chart Types you can set:
   - **Number of Sites**
   - **Number of Users per Site**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. To display a limited group of sites, enter the sites in the **Search Bar** fields.

Note The search bar fields use pattern matching with operators such as "contains". For example, "john" will match john_smith, john42, or big_john.

9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note These settings will stay in effect for all similar reports during your active login session.

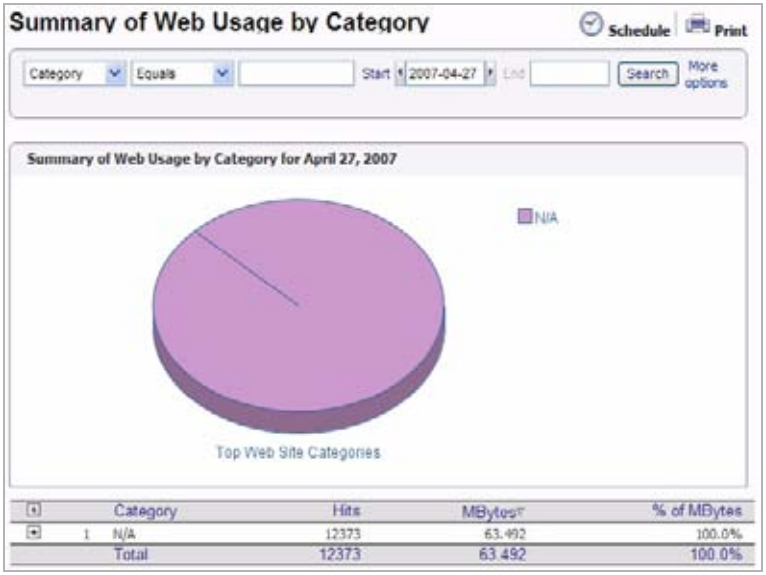
Viewing Web Usage By Category

The Web Usage By Category report displays a list of the top Web site categories, the number of hits to each category, the amount of data transferred, and the percentage of data transferred.

To view the By Category report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Usage** tree and click **By Category**. The By Category page displays.



4. The table contains the following information:
   - **Category**—the Web site category.
   - **Hits**—the number of hits to the Web site category.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred.
5. The ViewPoint Reporting Module shows yesterday's report and all Web site categories. To change the date of the report or Web site categories displayed, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

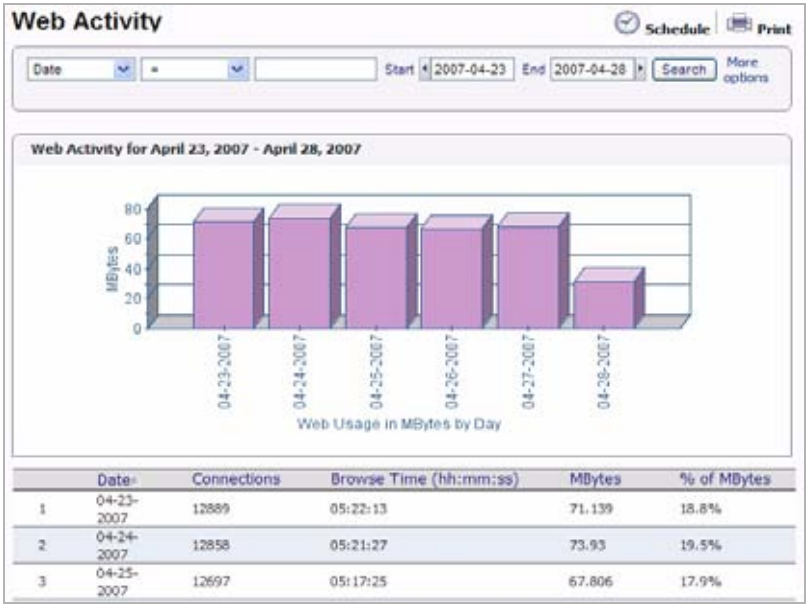
Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage Over Time

The Web Usage Over Time report displays the daily amount of HTTP bandwidth and browse time handled by a SonicWALL appliance or all SonicWALL appliances for the specified time period.

To view the Web Usage Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **Over Time**. The Web Activity page displays.



	Date	Connections	Browse Time (hh:mm:ss)	MBytes	% of MBytes
1	04-23-2007	12889	05:22:13	71.139	18.8%
2	04-24-2007	12858	05:21:27	73.93	19.5%
3	04-25-2007	12697	05:17:25	67.806	17.9%

4. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
5. The table contains the following information:

- **Date**—when the sample was taken.
- **Connections**—the number of connections or hits.
- **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.
- **MBytes**—the number of megabytes transferred.
- **% of MBytes**—the percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% of MBytes** field will display 25%.

6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Top Sites Over Time

The Top Sites Over Time report displays the most visited Web sites for the specified time period.

To view the Top Sites Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Usage** tree and click **Top Sites Over Time**. The Top Sites Over Time page displays.

4. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
5. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—the number of hits.
   - **MBytes**—the number of megabytes transferred.
   - **Category**—the Web site category.
   - **% of MBytes**—the percentage of megabytes transferred between this site, compared to all other HTTP traffic. For example, if 1,000,000 megabytes of data was transferred during the day and 500,000 megabytes was transferred between the appliance and Ebay, the **% of MBytes** field will display 50% and you have a problem.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Sites**

– **Rows per Screen**

See “Managing Report Settings” on page 154.

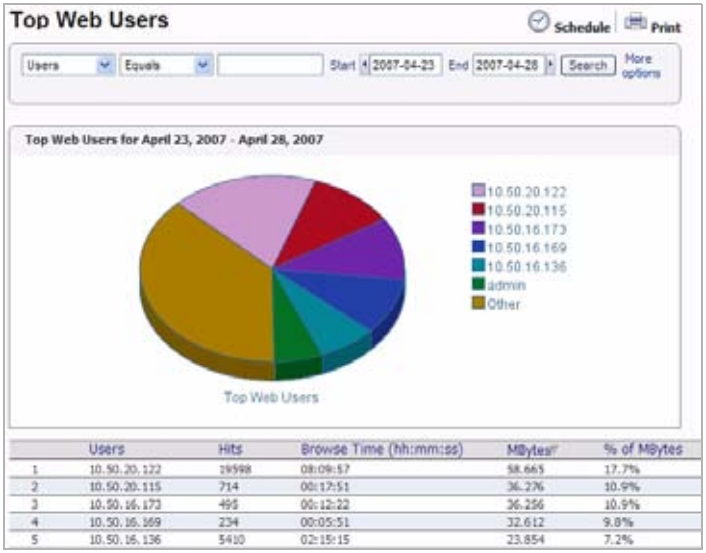
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Top Users Over Time

The Top Users Over Time report displays the top users of bandwidth and the amount of time they spent browsing the Internet for the specified time period. To view the Top Users Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The graph provides a graphical display of the percentage of bandwidth transferred by each of the top users over the specified time period.
5. The table contains the following information:

- **Site**—URL or IP address of the site.
- **Hits**—number of hits.
- **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.
- **MBytes**—number of megabytes transferred.
- **Category**—the category of the site.
- **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the period and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.

6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage By User Over Time

The By User Over Time report displays a list of all users, their top sites, the number of hits to each site, the time spent browsing, and the amount of data transferred for the specified time period.

To view the By User Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **By User Over Time**. The By User Over Time page displays.

4. The table contains the following information:
   - **User**—the IP address of the user.
   - **Hits**—number of hits to each Web site visited by the user.
   - **Browse Time**—number of hours, minutes, and seconds spent browsing non-job function-related sites on the Internet.
   - **MBytes**—number of megabytes transferred.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Number of Users**
   - **Number of Sites per User**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

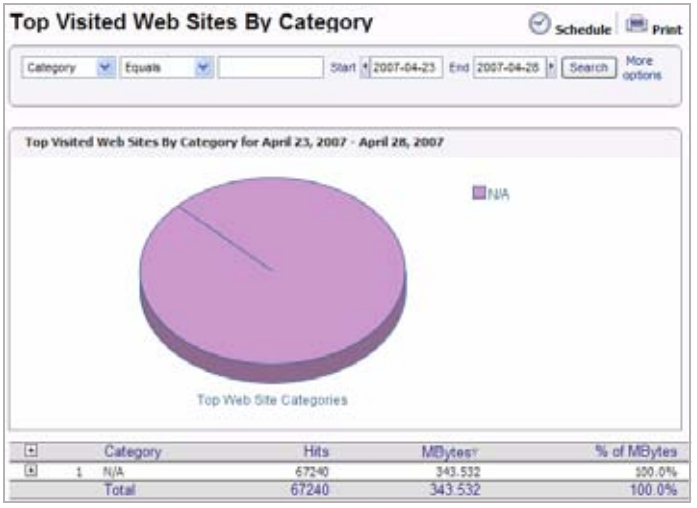
Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Usage By Category Over Time

The By Category Over Time report displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred for the specified time period.

To view the By Category Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Usage** tree and click **By Category Over Time**. The By User Over Time page displays.



4. The table contains the following information:
   - **Category**—the Web site category.
   - **Hits**—number of hits to each Web site visited by the user.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the period and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.

5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Note These settings will stay in effect for all similar reports during your active login session.

Viewing Web Filter Reports

Web filter reports provide information on the number of attempts that users made to access blocked Web sites through the selected SonicWALL appliance(s). These reports include Web sites blocked by the Content Filter List, customized keyword filtering, and domain name filtering.

Web filter reports can be used to view blocked site access attempts by the hour, day, or over a period of days. Additionally, you can view the users that most frequently attempt to access blocked sites and the most popular blocked sites.

Note All reports appear in the applianceUTM’s time zone.

Select from the following:

- “Viewing the Web Filter Summary Report” on page 210
- “Viewing the Web Filter Top Sites Report” on page 212
- “Viewing the Top Users that Try to Access Blocked Sites” on page 213
- “Viewing the Blocked Sites for Each User” on page 215
- “Viewing Blocked Sites Sorted By Site” on page 216

- “Viewing Blocked Sites Sorted By Category” on page 217
- “Viewing Blocked Site Attempts Over Time” on page 219
- “Viewing the Top Blocked Site Attempts Over Time” on page 220
- “Viewing the Top Blocked Site Users Over Time” on page 221
- “Viewing Blocked Sites for Each User Over Time” on page 222
- “Viewing Blocked Sites By Category Over Time” on page 223

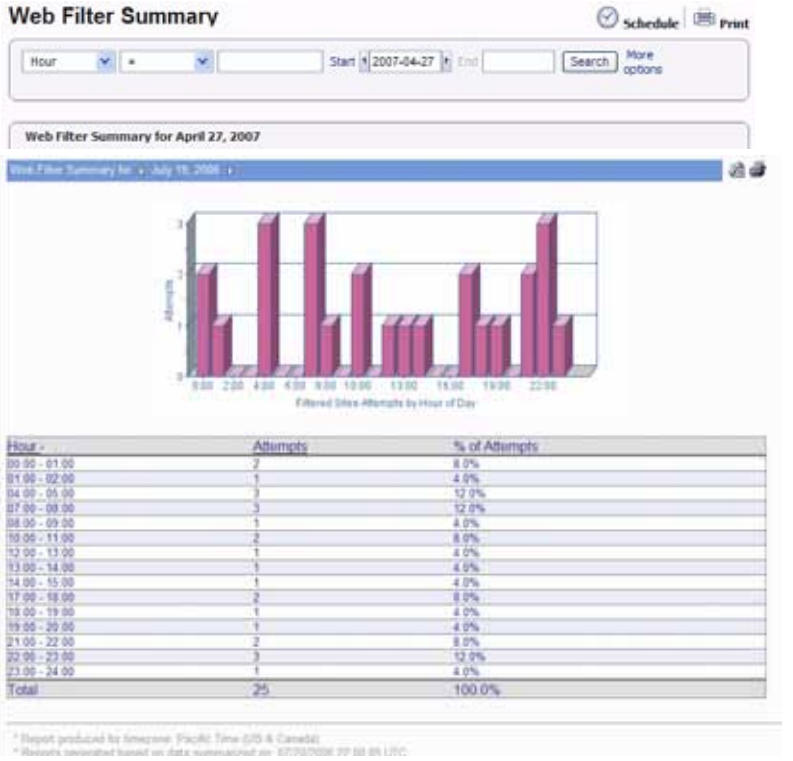
Viewing the Web Filter Summary Report

The Web Filter Summary report contains information on the number of times users attempt to access blocked sites for the specified day.

To view the Web Filter Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Web Filter** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of blocked sites that users attempted to access during each hour of the day.
5. The table contains the following information:
   - **Hour**—time when the sample was taken.
   - **Attempts**—the number of attempts to access blocked sites.
   - **% of Attempts**—the percentage of attempts during this hour, compared to the day. For example, if 100 attempts occurred during the day and 20 attempts occurred at the 12:00 time period, the **% of Attempts** field will display 20%.
6. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Web Filter Top Sites Report

The Web Filter Top Sites report displays the top blocked Web sites that users attempted to access on the specified date.

To view the Top Sites report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **Top Sites**. The Top Sites page displays.

4. The graph provides a display of the number of access attempts for each of the top twenty blocked Web sites.

5. The table contains the following information:
   - **Site**—the URL or IP address of the site.
   - **Attempts**—the number of attempts.
   - **Category**—the Web site category.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the day and 100 of those attempts were for www.badsite.com, its **% of Attempts** field will display 20%.
6. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Sites**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

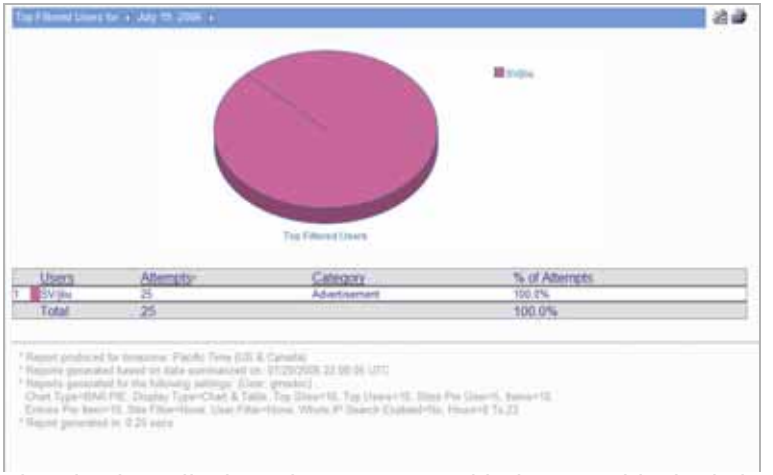
Viewing the Top Users that Try to Access Blocked Sites

The Web Filter Top Users report displays the users who made the most attempts to access blocked sites on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.

2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the top users with the most blocked site attempts.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—the number of attempts.
   - **Category**—the Web site category.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the day and 250 of those attempts were made by a single user, that user's **% of Attempts** field will display 50%.
6. By default, ViewPoint Reporting shows yesterday's report, a pie chart, and the ten top users. To change these settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table** or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing the Blocked Sites for Each User

The Web Filter By User report displays the top blocked Web sites that each user attempted to access on the specified date.

To view the Web Filter By User report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **By User**. The By User page displays.

4. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Attempts**—the number of attempts the user made to access each Web site.
5. You can navigate directly from the **Web Filter > By User** page to a **Web Filter > By Site** page detailing the information of the site the user has been browsing. Click the **Plus** sign to the left of the **User** name or IP address to show details, and then hover the mouse over a site. A sticky tooltip will display with a link to the corresponding site's report page.
6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change these settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:

- **Number of Users**
- **Number of Sites per User**
- **Rows per Screen**

See “Managing Report Settings” on page 154.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected settings.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing Blocked Sites Sorted By Site

The Web Filter By Site report displays the top blocked Web sites that were accessed by users.

To view the Web Filter By Site report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **By Site**. The By Site page displays.

4. The table contains the following information:
   - **Site**—the top five sites visited by the user.
   - **Attempts**—the number of attempts the user made to access each Web site.
   - **Category**—the Web site category.

5. You can navigate directly from the **Web Filter > By Site** page to a **Web Filter > By User** page detailing the information of the users who have been browsing the site. Click the Plus sign to the left of the Site to show details, and then hover the mouse over a user. A sticky tooltip will display with a link to the corresponding user report page.
6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change these settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Number of Users per Site:
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. Search for Web site addresses in the Search Bar fields.
9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

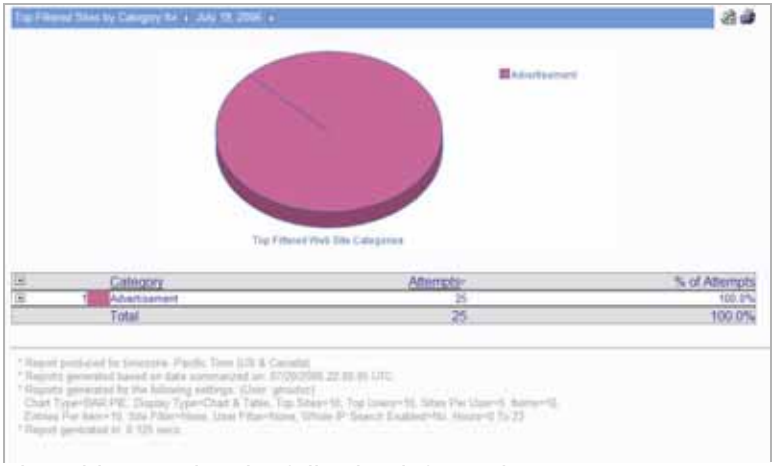
Viewing Blocked Sites Sorted By Category

The Web Filter By Category report displays the top categories of Web sites that were accessed by users.

To view the Web Filter By Category report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Filter** tree and click **By Category**. The By Site page displays.



4. The table contains the following information:
   - **Category**—the Web site category.
   - **Attempts**—the number of attempts the user made to access each Web site.
   - **% of Attempts**—the percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the day and 250 of those attempts were made by a single user, his **% of Attempts** field will display 50%.
5. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change these settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Blocked Site Attempts Over Time

The Web Filter Over Time report displays the number of attempts that were made to access blocked Web sites for the specified time period.

To view the Web Filter Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **Over Time**. The Over Time page displays.

Date	Attempts	% of Attempts
07-14-2006	9	7.9%
07-15-2006	24	21.1%
07-16-2006	21	18.4%
07-17-2006	13	11.4%
07-18-2006	22	19.3%
07-19-2006	25	21.9%
Total	114	100.0%

4. The bar graph displays the number of attempts that were made to access blocked Web sites during each day of the specified time period.
5. The table contains the following information:
   - **Date**—the day when the sample was taken.
   - **Attempts**—the number of attempts to access blocked Web sites.
   - **% of Attempts**—the percentage of attempts to access the blocked site on the day, compared to the time period. For example, if 5,000 attempts were made during the time period and 500 were made on one day, its **% of Attempts** field will display 10%.
6. To change date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

See “Managing Report Settings” on page 154.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

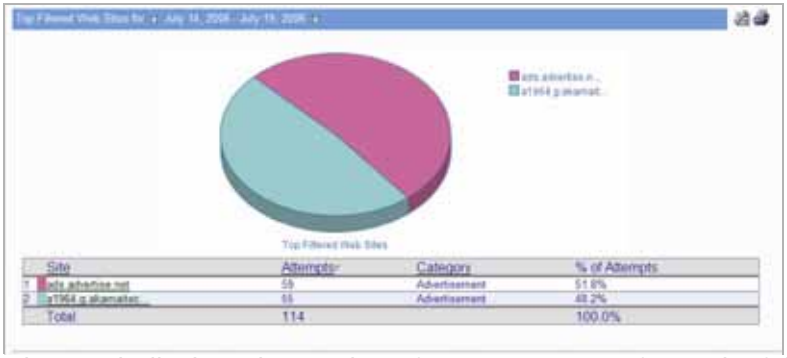
Note These settings will stay in effect for all similar reports during your active login session.

Viewing the Top Blocked Site Attempts Over Time

The Top Sites Over Time report displays the top blocked Web sites for the specified time period.

To view the Web Filter Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **Top Sites Over Time**. The Top Sites Over Time page displays.



4. The graph displays the number of access attempts for each of the top blocked Web sites during the specified time period.
5. The table contains the following information:
   - **Site**—the URL or IP address of the site.
   - **Attempts**—the number of attempts.
   - **Category**—the Web site category.
   - **% of Attempts**—the percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the period and 100 of those attempts were for www.badsite.com, its **% of Attempts** field will display 20%.

6. To change date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Sites**
   - **Rows per Screen**

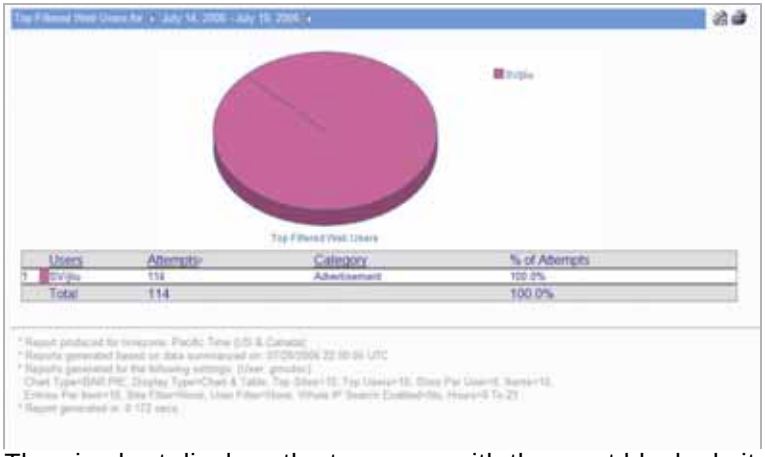
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top Blocked Site Users Over Time

The Web Filter Top Users Over Time report displays the users who made the most attempts to access blocked sites during the specified time period.

To view the Top Users Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the top users with the most blocked site attempts.

5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—the number of attempts.
   - **Category**—the Web site category.
   - **% of Attempts**—the percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the period and 250 of those attempts were made by a single user, his **% of Attempts** field will display 50%.
6. To change date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Sites**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Blocked Sites for Each User Over Time

The Web Filter By User report displays the top blocked Web sites that each user attempted to access during the specified time period.

To view the By User Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Web Filter** tree and click **By User Over Time**. The By User Over Time page displays.

4. The table contains the following information:
   - **User**—the IP address or name of the user.
   - **Attempts**—the number of attempts the user made to access each Web site.
5. To change date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

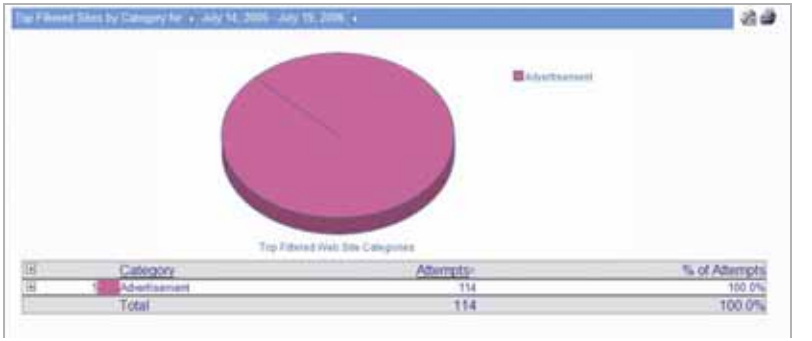
Note These settings will stay in effect for all similar reports during your active login session.

Viewing Blocked Sites By Category Over Time

The Web Filter By Category Over Time report displays the top categories that users attempted to access.

To view the By Category Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Web Filter** tree and click **By Category Over Time**. The By Category Over Time page displays.



4. The table contains the following information:
   - **Category**—the Web site category.
   - **Attempts**—number of attempts the user made to access each Web site.
   - **% of Attempts**—the percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the period and 250 of those attempts were made by a single user, his **% of Attempts** field will display 50%.
5. To change date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing File Transfer Protocol Reports

FTP usage reports provide information on the amount of FTP usage that occurs through the selected SonicWALL appliance(s).

FTP usage reports can be used to view FTP bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of FTP bandwidth.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of FTP traffic occurs during peak times, you might need more bandwidth, you might need to upgrade network equipment, or you might ask employees to use compression or transfer large files during non-peak times.

Note All reports appear in the appliance's time zone.

Select from the following:

- "Viewing the FTP Summary Report" on page 225
- "Viewing the Top FTP Sites By User" on page 227
- "Viewing FTP Bandwidth Usage Over Time" on page 228
- "Viewing the Top Users of FTP Bandwidth Over Time" on page 230

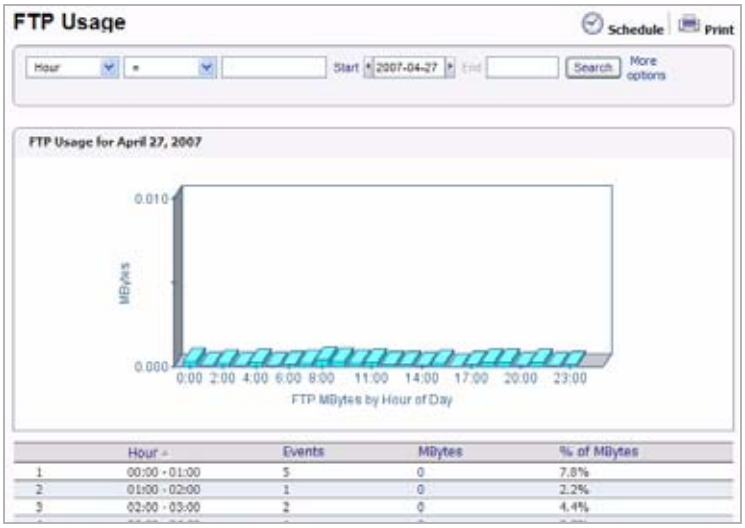
Viewing the FTP Summary Report

The FTP Summary report contains information on the amount of FTP bandwidth handled by a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the FTP Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **FTP Usage** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the amount of FTP bandwidth transferred during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—the number of FTP events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of FTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date or other report settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart

   See "Managing Report Settings" on page 154.

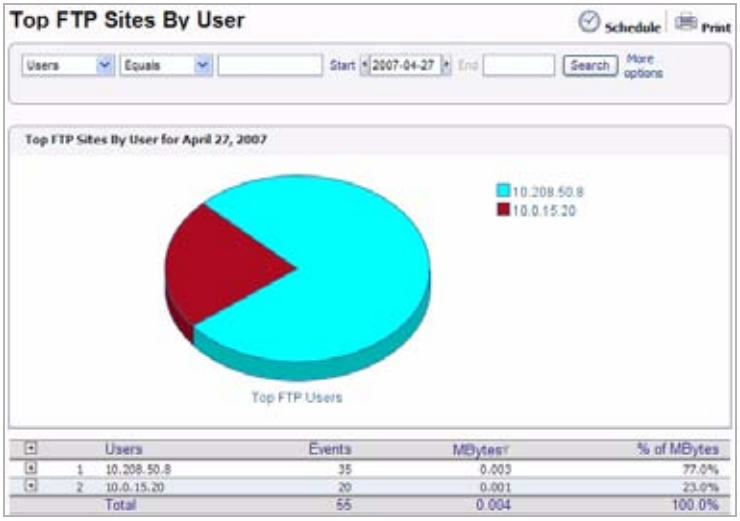
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Top FTP Sites By User

The By User report displays the users who used the most FTP bandwidth on the specified date.

To view the By User report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **FTP Usage** tree and click **By User**. The By User page displays.



4. The pie chart displays the percentage of bandwidth used by each user. To view the sites visited by each user, expand the user's site tree (indicated by a '+' sign).
5. The table contains the following information:

- **Users**—the IP address of the user.
- **Events**—the number of FTP Events.
- **MBytes**—the number of megabytes transferred.
- **% of MBytes**—the percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of FTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.

6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change these settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Number of Sites per User**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. To display a limited group of users, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as "contains". For example, "john" will match john_smith, john42, or big_john.

9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

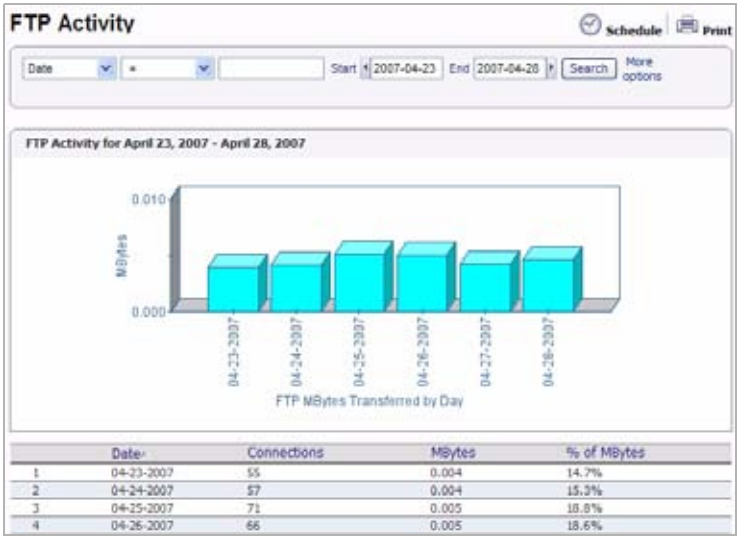
Viewing FTP Bandwidth Usage Over Time

The FTP Usage Over Time report displays the daily amount of FTP bandwidth handled by a SonicWALL appliance or all SonicWALL appliances for the specified time period.

To view the FTP Usage Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **FTP Usage** tree and click **Over Time**. The FTP Activity page displays.



4. The bar graph displays the amount of FTP bandwidth transferred during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—the number of FTP connections.
   - **MBytes**—the number of megabytes transferred.
   - **% of Usage**—the percentage of megabytes transferred during this day, compared to the time period. For example, if 10,000 megabytes of FTP data was transferred during the time period and 2,500 megabytes of FTP data was transferred on one day, the **% of Usage** field will display 25%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top Users of FTP Bandwidth Over Time

The By Users Over Time report displays the users who used the most FTP bandwidth for the specified time period.

To view the By Users Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **FTP Usage** tree and click **By Users Over Time**. The By Users Over Time page displays.

4. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—the number of FTP Events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10000 megabytes of data was transferred during the period and 2000 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Number of Sites per User**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. To display a limited group of users, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Mail Usage Reports

Mail usage reports provide information on the amount of mail usage that occurs through the selected SonicWALL appliance(s).

Mail usage reports can be used to view mail bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of mail bandwidth.

Note Mail usage reports include SMTP, POP3, and IMAP traffic.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of mail traffic occurs during peak times, you might want to take some of the following actions:

- Add bandwidth
- Upgrade network equipment
- Ask employees to use compression or transfer large files during non-peak times
- Ask employees to place large files on an FTP site rather than sending them as mail attachments.

Note All reports appear in the appliance's time zone.

Select from the following:

- To view a summary of the daily mail usage, see "Viewing the Mail Usage Summary Report" on page 232.
- To view the users who consume the most mail bandwidth, see "Viewing the Top Users of Mail Bandwidth" on page 234.
- To view mail usage over a period of time, see "Viewing Mail Usage Over Time" on page 235.
- To view the users who consume the most mail bandwidth over time, see "Viewing the Top Users of Mail Bandwidth Over Time" on page 237.

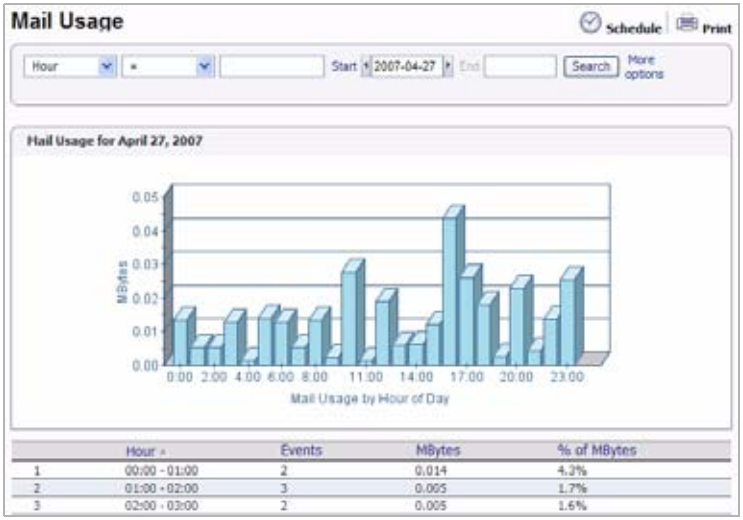
Viewing the Mail Usage Summary Report

The Mail Usage Summary report contains information on the amount of mail handled by a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the Mail Usage Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Mail Usage** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the amount of mail sent and received during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—the number of mail events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred during this hour, compared to the day. For example, if 10,000 megabytes of mail was transferred during the day and 1,000 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report or the report display settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

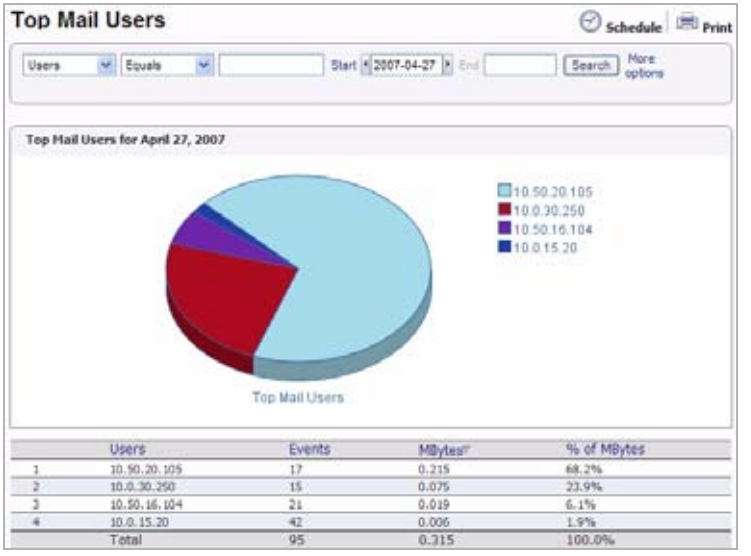
   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Top Users of Mail Bandwidth

The Top Users report displays the users who sent and received the most mail on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Mail Usage** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of mail sent and received by the top mail users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—the number of mail messages sent and received.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10000 megabytes of data was transferred during the day and 2000 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.

6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change the date of the report or the report display settings, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

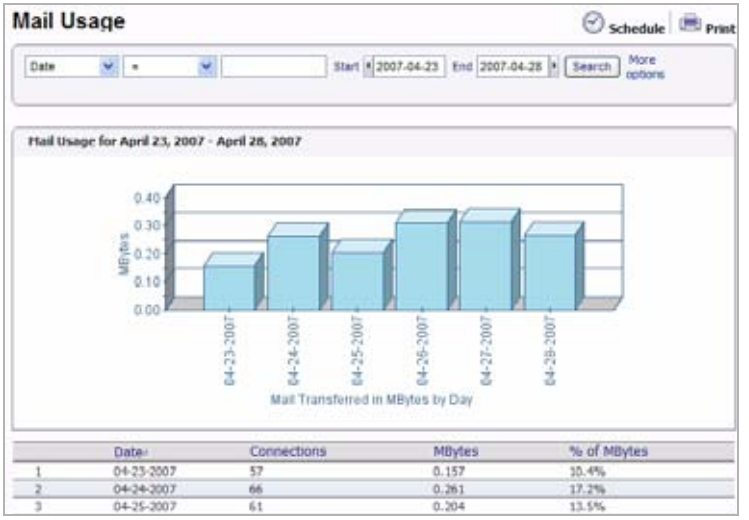
Viewing Mail Usage Over Time

The Mail Usage Over Time report displays the daily amount of mail handled by a SonicWALL appliance or all SonicWALL appliances for the specified time period.

To view the Mail Usage Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Mail Usage** tree and click **Over Time**. The Over Time page displays.



4. The bar graph displays the amount of mail sent and received during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—the number of mail messages.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10000 megabytes of data was transferred during the day and 2000 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type: Area, Bar** or **Plot chart**

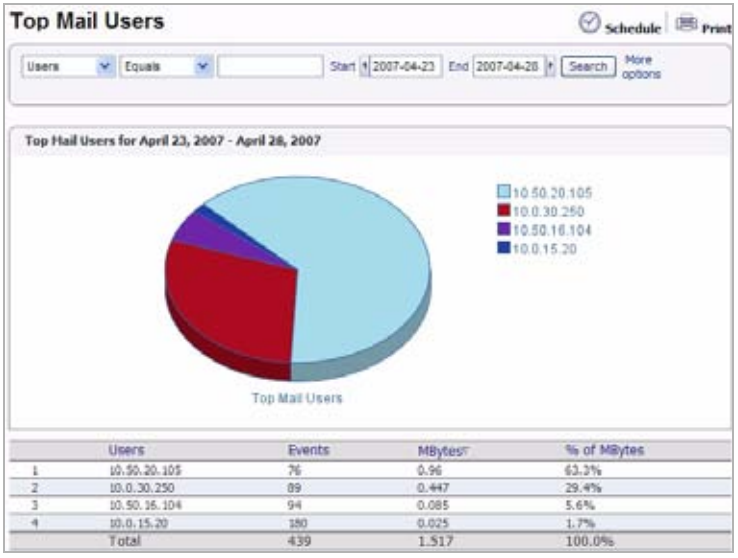
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top Users of Mail Bandwidth Over Time

The Top Users Over Time report displays the users who sent and received the most mail during the specified time period.

To view the Top Users Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Mail Usage** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the percentage of mail sent and received by the top mail users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—the number of mail messages sent and received.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.

6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. To display a limited group of users, use the Search Bar fields.

   The search bar fields use pattern matching with operators such as "contains". For example, "john" will match john_smith, john42, or big_john.
9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing VPN Usage Reports

VPN Usage reports provide information on the amount of VPN usage that occurs through the selected SonicWALL appliance(s).

VPN Usage reports can be used to view VPN usage by the hour, day, or over a period of days. Additionally, you can view the top users of VPN.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of VPN traffic occurs, you might need to add bandwidth, upgrade network equipment, or reconfigure the VPN network.

Note All reports appear in the appliance's time zone.

Select from the following:

- To view a summary of the daily VPN bandwidth usage, see "Viewing the VPN Usage Summary Report" on page 239.
- To view the users who consume the most VPN bandwidth, see "Viewing the Top VPN Users" on page 241.
- To view VPN bandwidth usage over a period of time, see "Viewing VPN Usage Over Time" on page 242.

- To view the users who consume the most VPN bandwidth over time, see “Viewing VPN Usage Over Time” on page 242.
- To view the users who consume the most VPN bandwidth over time, see “Viewing the Top VPN Users Over Time” on page 243.
- To view VPN usage by policy, see “Viewing VPN Usage By Policy” on page 245.
- To view VPN usage by policy over time, see “Viewing the Top VPN Policies Over Time” on page 246.
- To view hourly VPN usage by policy, see “Viewing Hourly VPN Usage By Policy” on page 248.
- To view VPN services usage, see “Viewing the VPN Services Summary Report” on page 249.

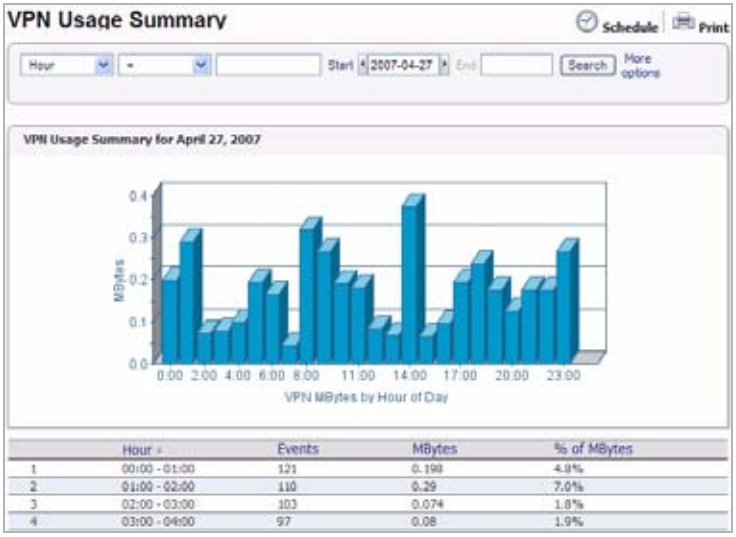
Viewing the VPN Usage Summary Report

The VPN Usage Summary report contains information on the number of VPN connections made through a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the VPN Usage Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **VPN Usage** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of VPN connections made during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—the number of mail events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

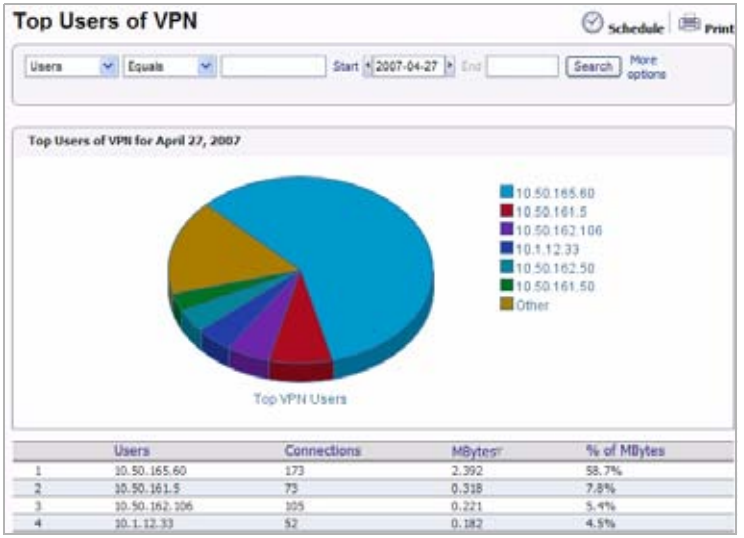
   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top VPN Users

The Top Users report displays the users who made the most VPN connections on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the VPN connections for the top VPN users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—the number of VPN connections.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

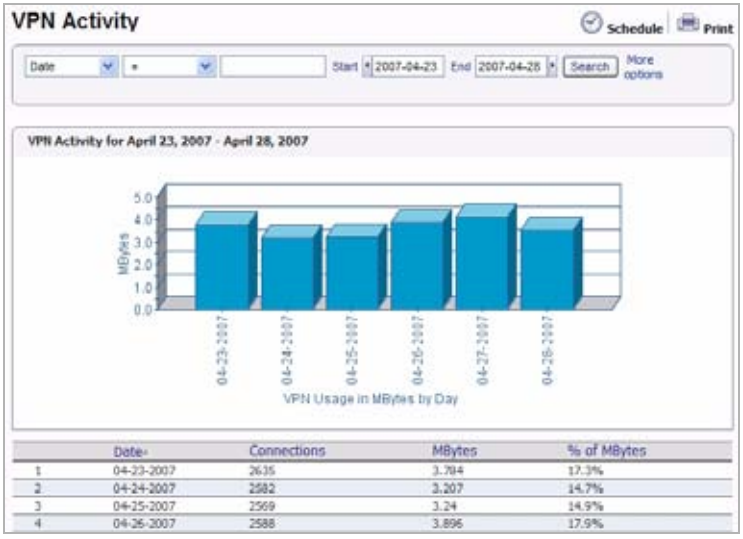
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing VPN Usage Over Time

The VPN Usage Over Time report displays the daily number of VPN connections made through a SonicWALL appliance or all SonicWALL appliances during the specified time period.

To view the VPN Usage Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **Over Time**. The Over Time page displays.



4. The bar graph displays the number of VPN connections made during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—the number of connections.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

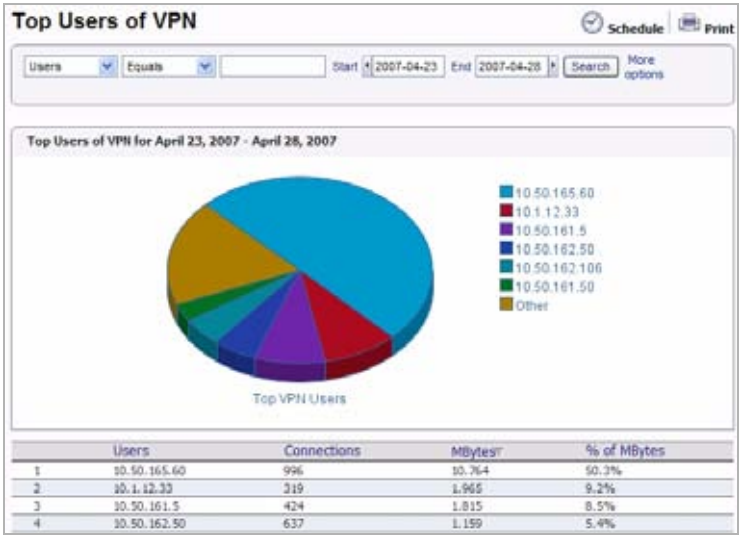
Viewing the Top VPN Users Over Time

The Top Users report displays the users who made the most VPN connections for the specified time period.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **VPN Usage** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the VPN connections for the top VPN users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—the number of VPN connections.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.

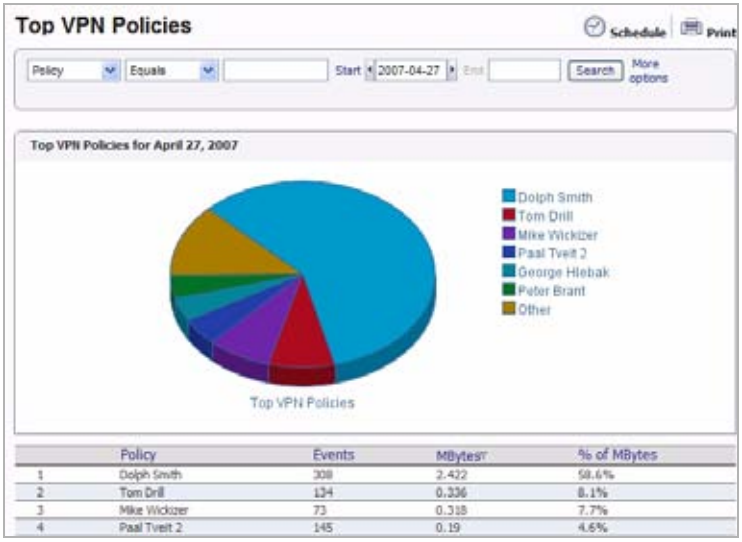
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing VPN Usage By Policy

The VPN Usage By Policy report contains information on VPN usage for a SonicWALL appliance, organized by policy.

To view the VPN Usage By Policy report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Policy**. The By Policy page displays.



4. The pie chart displays the amount of data transferred for each policy.
5. The table contains the following information:
   - **Policy**—the name of the policy.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred for this policy, compared to all other policies. For example, if a total of 10,000 megabytes was transferred and 2,500 megabytes was transferred for one policy, the **% of Usage** field will display 25%.

6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

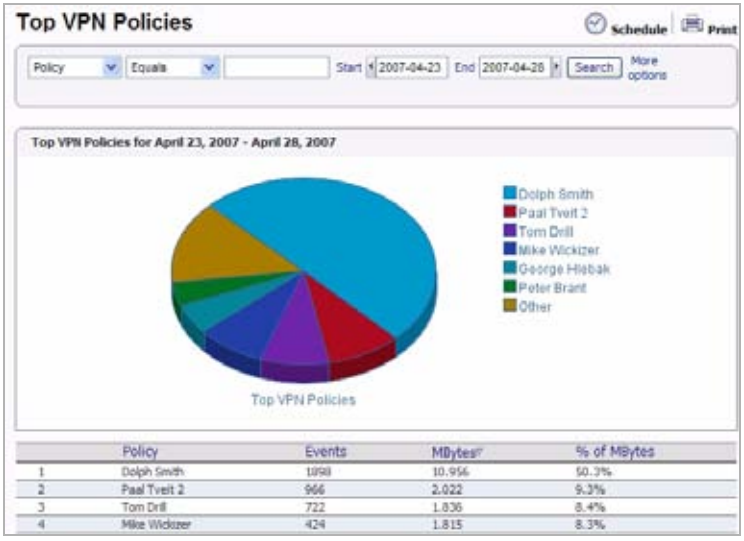
Viewing the Top VPN Policies Over Time

The By Policy Over Time report displays the top VPN Policies for the specified time period.

To view the By Policy Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **VPN Usage** tree and click **By Policy Over Time**. The By Policy Over Time page displays.



4. The pie chart displays the VPN connections for the top policies.
5. The table contains the following information:
   - **Policy**—the name of the policy.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred for this policy, compared to all other policies for the period. For example, if a total of 100,000 megabytes was transferred and 3,000 megabytes was transferred for one policy, the **% of MBytes** field will display 3%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Hourly VPN Usage By Policy

The VPN Usage By Policy Hourly report contains information on hourly VPN usage for a SonicWALL appliance, organized by policy.

To view the VPN Usage By Policy Hourly report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Policy Hourly**. The By Policy Hourly page displays.

4. The table contains the following information:
   - **Hour**—the period of time.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
5. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart
   - **Hour Begin**
   - **Hour End**

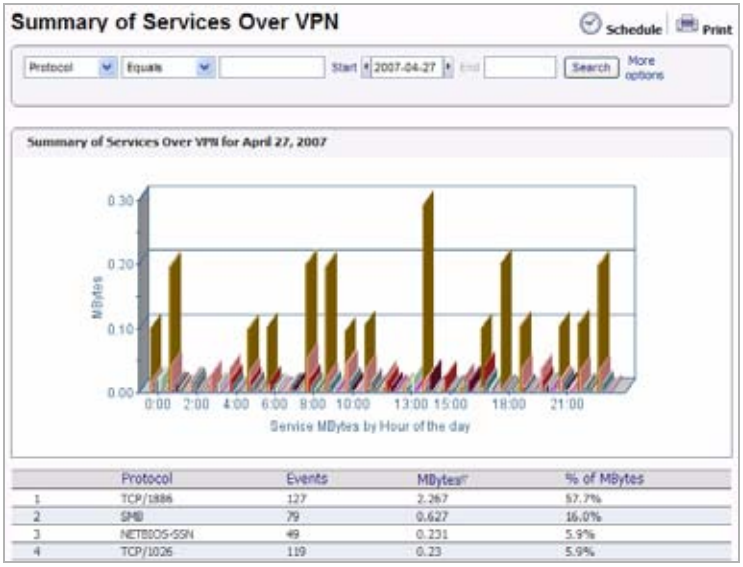
   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the VPN Services Summary Report

The Services Summary report displays the amount of traffic handled by each service during each hour of the specified day.

To view the Services Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Service**. The By Service page displays.



4. The bar graph displays the amount of bandwidth used by each service during each hour of the day.

5. The table contains the following information:
   - **Protocol**—the service.
   - **Events**—the number of events or “hits.”
   - **MBytes**—the number of megabytes.
   - **% of MBytes**—the percentage of megabytes transferred by this service on the selected day, compared to all other services. For example, if 1,000 megabytes were transferred and 900 megabytes were handled by the HTTP service, the **% of Mbytes** field will display 90%.
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing Attacks Reports

Attacks reports show the number of attacks that were directed at or through the selected SonicWALL appliance(s). These include denial of service attacks, intrusions, probes, and all other malicious activity directed at the SonicWALL appliance or computers on the LAN or DMZ.

Note All reports appear in the appliance’s time zone.

Select from the following:

- To view a summary of the attacks, see “Viewing the Attack Summary Report” on page 251.
- To view the attacks by attack category, see “Viewing the Attacks By Category” on page 253.
- To view the attacks by source IP address, see “Viewing the Errors Report” on page 254.
- To view a summary of the errors and exceptions, see “Viewing the Errors Report” on page 254.
- To view attacks over a period of time, see “Viewing Attack Reports Over Time” on page 256.
- To view errors and exceptions over a period of time, see “Viewing Errors Over Time” on page 258.

Viewing the Attack Summary Report

The Attack Summary report contains information on the number of attacks attempted on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the Attack Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Attacks** tree and click **Summary**. The Summary page displays.

4. The bar graph displays the number of attacks attempted during each hour of the day. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Attacks**—the number of attack attempts.
   - **% of Attacks**—the percentage of attacks during this hour, compared to the day. For example, if 1,000 attacks occurred during the day and 100 attacks occurred during the 2:00 time period, the **% of Attacks** field will display 10%.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

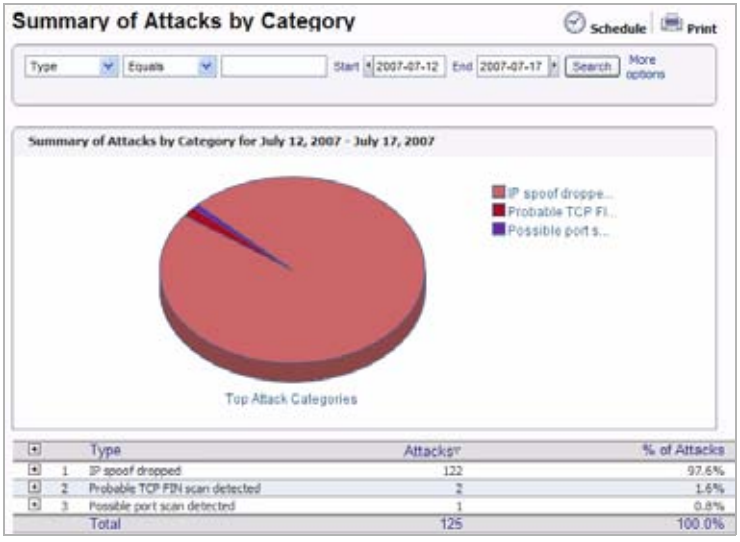
   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Attacks By Category

The Attacks By Category report displays the attacks that occurred on the specified date, sorted by category.

To view the Attacks By Category report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Attacks** tree and click **By Category**. The By Category page displays.



4. The pie chart displays the percentage of each type of attack. To view source and destination information on the individual attacks, expand the category tree (indicated by a '+' sign).
5. The table contains the following information:
   - **Type**—the type of attack
   - **Source**—the IP address of the source
   - **Destination**—the IP address to the destination
     Click the highlighted source or destination IP address to access the Who is Source Website.

- **Attacks**—the number of attacks
- **% of Attacks**—the percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field will display 10%.

6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top categories. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.
9. These settings will stay in effect for all similar reports during your active login session.

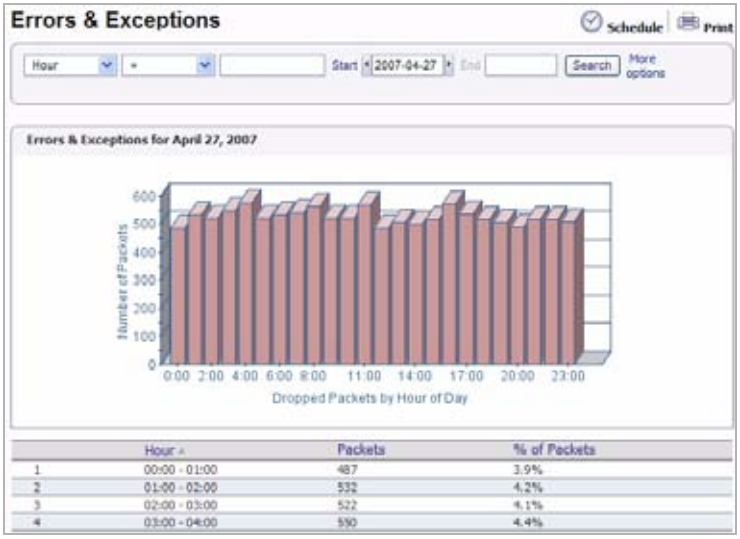
Viewing the Errors Report

The Errors Summary report contains information on the number of dropped packets on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the Errors report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Attacks** tree and click **Errors**. The Errors page displays.



4. The bar graph displays the packets that were dropped during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Packets**—the number of dropped packets.
   - **% of Packets**—the percentage of packets dropped during this hour, compared to the day. For example, if 1,000 packets were dropped during the day and 100 packets were dropped during the 1:00 time period, the **% of Packets** field will display 10%.
6. The ViewPoint Reporting Module shows yesterday's report.To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

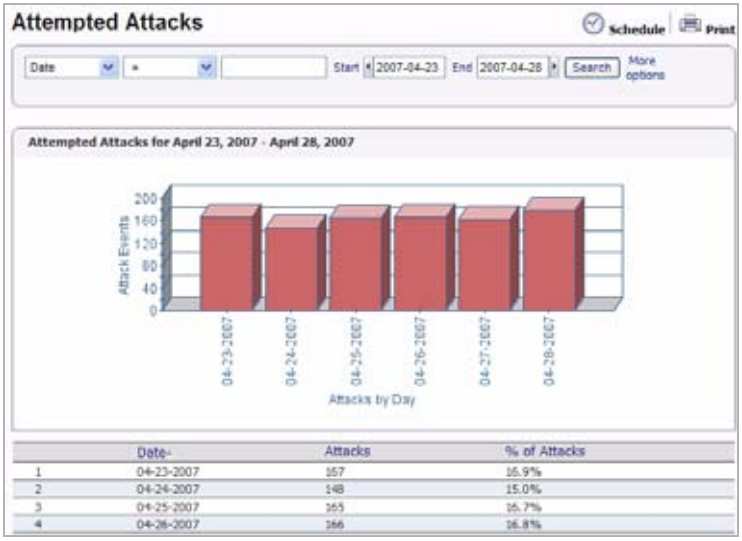
   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Attack Reports Over Time

The Attacks Over Time report displays the daily number of attempted attacks during the specified time period.

To view the Attacks Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Attacks** tree and click **Attacks Over Time**. The Attacks Over Time page displays.



4. The bar graph displays the number of attacks attempted each day of the time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Attacks**—the number of attacks.
   - **% of Attacks**—the percentage of attacks on this day, compared to the time period. For example, if 10,000 attacks occurred during the time period and 1,000 attacks occurred on Thursday, its **% of Attacks** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

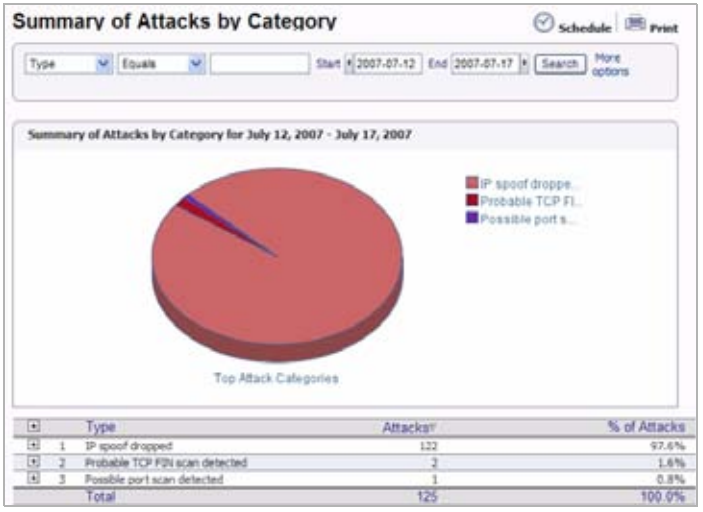
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Attacks By Category Over Time

The Categories Over Time report displays the number of attacks in each attack category during the specified time period.

To view the Categories Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Attacks** tree and click **Categories Over Time**. The Categories Over Time page displays.



4. The bar graph displays the number of attacks attempted each day of the specified time period. To view source and destination information on the individual attacks, expand the category tree (indicated by a ‘+’ sign).
5. The table contains the following information:
   - **Type**—the type of attack
   - **Source**—the IP address of the source

- **Destination**—the IP address to the destination
  Click the highlighted source or destination IP address to access the Whois Source Website.
- **Attacks**—the number of attacks
- **% of Attacks**—the percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field will display 10%.

6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

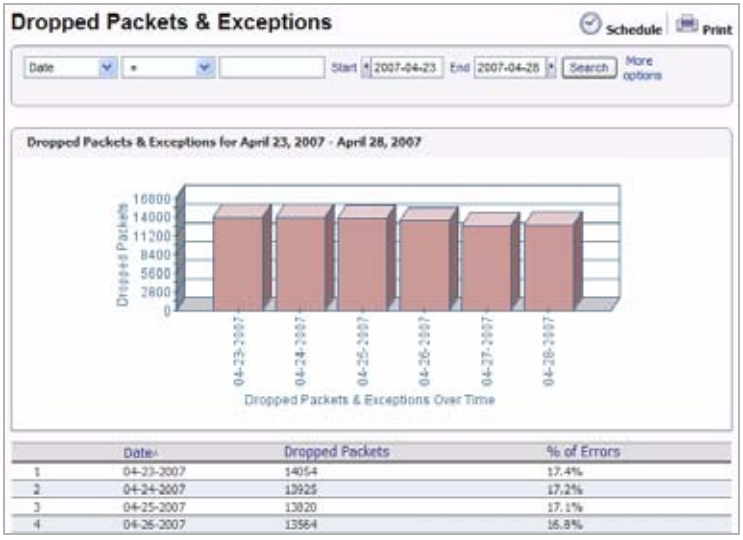
Viewing Errors Over Time

The Errors Over Time report displays the number of errors during the specified time period.

To view the Errors Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Attacks** tree and click **Errors Over Time**. The Dropped Packets & Exceptions page displays.



4. The bar graph displays the number of packets that were dropped during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Dropped Packets**—the number of dropped packets.
   - **% of Errors**—the percentage of dropped packets on this day, compared to the time period. For example, if 10,000 packets were dropped during the time period and 1,000 packets were dropped on Wednesday, its **% of Attacks** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Virus Attacks Reports

Virus Attacks reports show the number of virus attacks that were directed at or through the selected SonicWALL appliance(s).

Note All reports appear in the appliance's time zone.

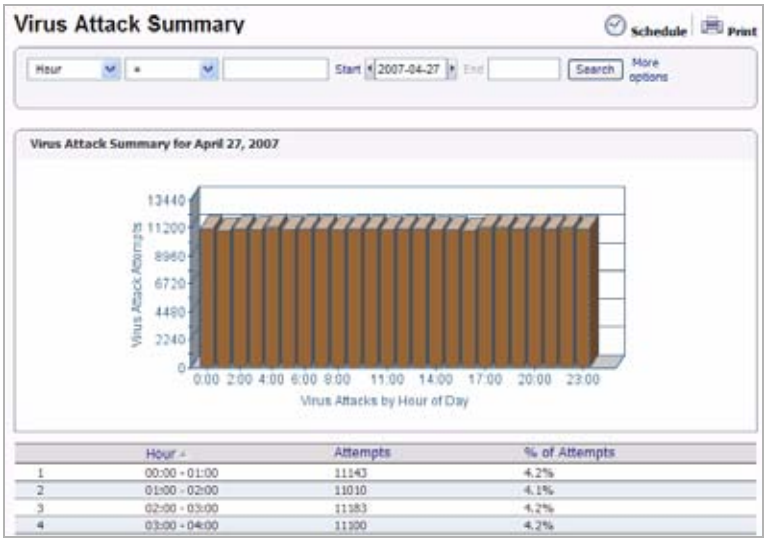
If the selected appliance is not licensed for SonicWALL Gateway Anti-Virus, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all viruses and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Gateway Anti-Virus and other subscription services.

Select from the following reports:

- To view the top virus, see "Viewing the Top Viruses By Attack Attempts Report" on page 262.
- To view the virus attacks by top destinations, see "Viewing the Virus Attack Attempts Report" on page 263.

- To view virus attacks over time, see “Viewing the Virus Attack Attempts Report” on page 263.
- To view virus attacks over a period of time, see “Viewing the Virus Attacks By User Report” on page 265.
- To view virus attacks by top destinations over time, see “Viewing Anti-Spyware Reports” on page 266.

9. Expand the **Virus Attacks** tree and click **Summary**. The Summary page displays



10. The bar graph displays the number of virus attacks attempted during each hour of the day. The table contains the following information:
    - **Hour**—the hour of the day for which the summary is provided.
    - **Attempts**—the number of times the virus attempted to infect the device during a pre-set time interval (the hour of the day is the default).
    - **% of Attempts**—the percent of attempts the current virus entry comprises as a portion of the aggregate number of virus attempts on the device during a pre-set time interval (the hour of the day is the default).
11. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
12. Under Report Display Settings you can set:

- **Display Type**: **Chart and Table**, or **Table Only**
- **Chart Type**: **Area**, **Bar** or **Plot** chart

See “Managing Report Settings” on page 154.

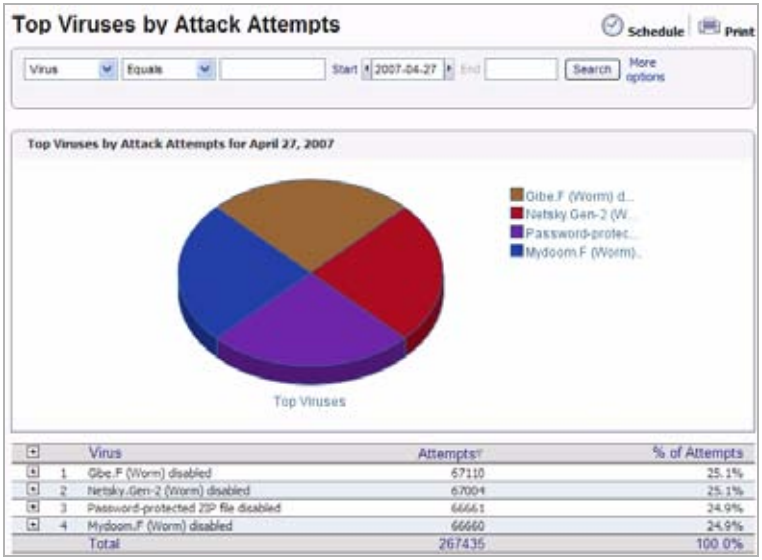
13. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top Viruses By Attack Attempts Report

The Top Viruses By Attack Attempts report displays the top viruses for the specified date.

To view the Top Viruses, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Virus Attacks** tree and click **By Virus**. The Top Viruses By Attack Attempts page displays.



4. The pie chart displays the percentage of virus attacks attempted in a given day.
5. The table contains the following information:
   - **Virus**—the name of the virus.
   - **Attempts**—the number of attack attempts.

- **% of Attempts**—the percentage of attempts as compared to the day.

6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

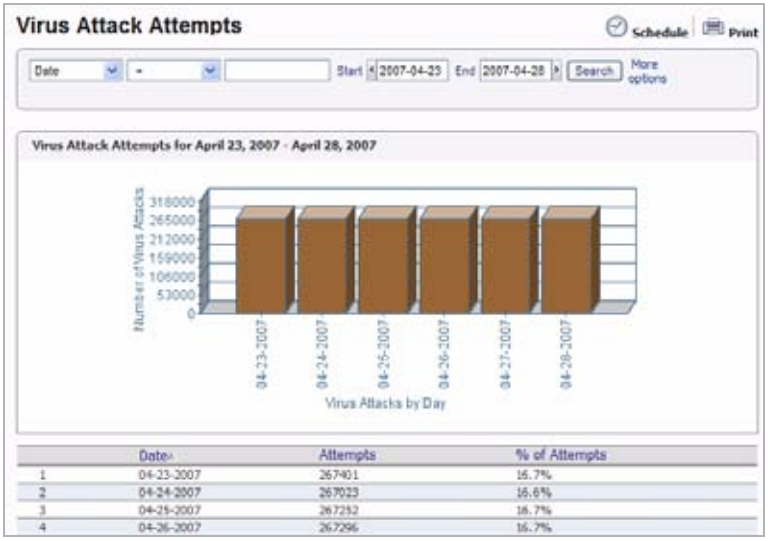
Viewing the Virus Attack Attempts Report

The Virus Attack Attempts report displays the number of virus attempts over the specified time range.

To view the Virus Attack Attempts report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Virus Attacks** tree and click **Over Time**. The Virus Attack Attempts page displays.



4. The bar graph displays the number of virus attempts that were made during each day over a specified time period.
5. The table contains the following information:
   - **Date**—the date of when the sample was taken.
   - **Attempts**—the number of attempted virus attacks.
   - **% of Attempts**—the percentage of attempted virus attacks in a day compared to the time period. For example, if 5,000 attempts were made during the time period and 500 were made on one day, its **% of Attempts** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

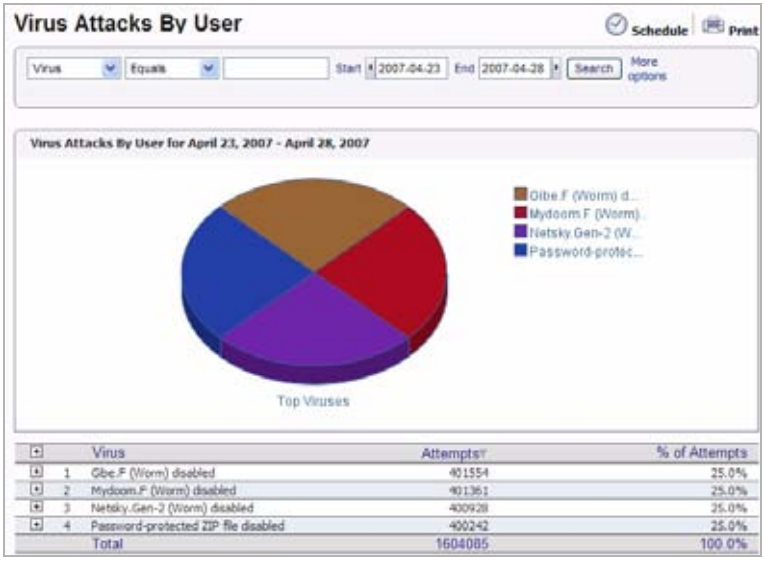
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Virus Attacks By User Report

The Virus Attacks By User report displays the number of virus attack attempts over the specified time range.

To view the Virus Attacks By User report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Virus Attacks** tree and click **By Viruses Over Time**. The Virus Attacks By User page displays.



4. The pie chart displays the percentage of virus attacks attempted in a given day.
5. The table contains the following information:
   - **Virus**—the name of the virus.
   - **Attempts**—the number of attack attempts.
   - **% of Attempts**—the percentage of attempts compared to the day.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

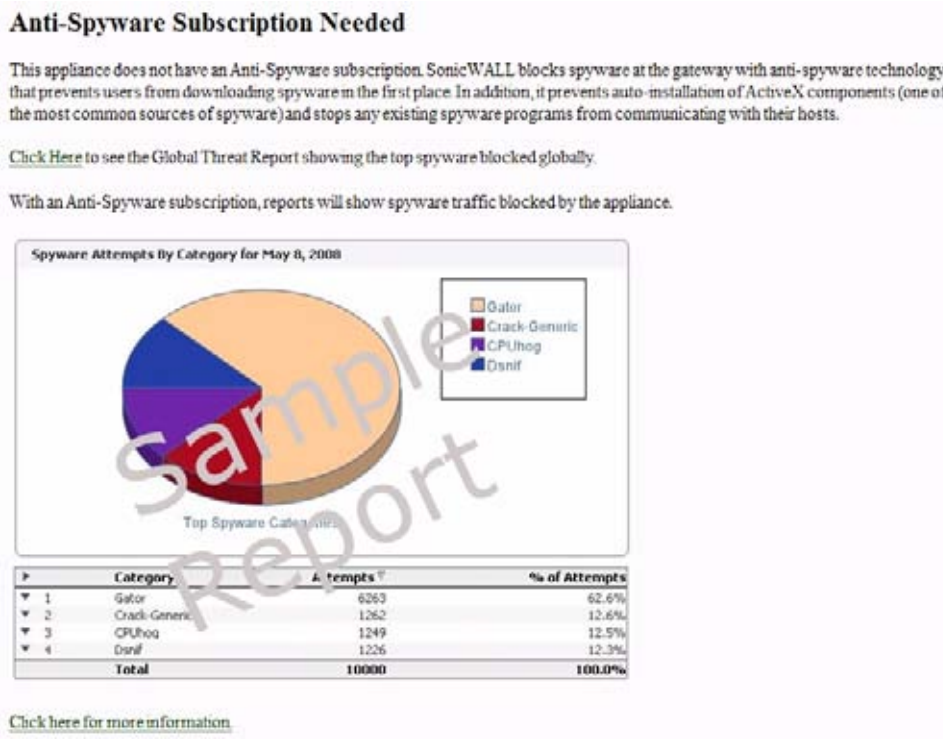
Viewing Anti-Spyware Reports

SonicWALL Anti-Spyware is included within the SonicWALL Gateway Anti-Virus (GAV), Anti-Spyware and Intrusion Prevention Service (IPS) unified threat management (UTM) solution. SonicWALL UTM delivers a comprehensive, real-time gateway security solution for your entire network.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interface enable administrators to configure a custom set of detection or prevention policies tailored to their specific network

environment. Network administrators can create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.

If the selected appliance is not licensed for SonicWALL Anti-Spyware, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all spyware and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Anti-Spyware and other subscription services.


Anti-Spyware Subscription Needed
This appliance does not have an Anti-Spyware subscription. SonicWALL blocks spyware at the gateway with anti-spyware technology that prevents users from downloading spyware in the first place. In addition, it prevents auto-installation of ActiveX components (one of the most common sources of spyware) and stops any existing spyware programs from communicating with their hosts.
Click Here to see the Global Threat Report showing the top spyware blocked globally.
With an Anti-Spyware subscription, reports will show spyware traffic blocked by the appliance.
Spyware Attempts By Category for May 8, 2008
Gator
Crack-Generic
CPUhog
Dsnif
Sample Report
Top Spyware Categories
Category
Attempts
% of Attempts
1 Gator 6263 62.6%
2 Crack-Generic 1262 12.6%
3 CPUhog 1249 12.5%
4 Dsnif 1226 12.3%
Total 10000 100.0%
Click here for more information

See the following sections to view Anti-Spyware reports:

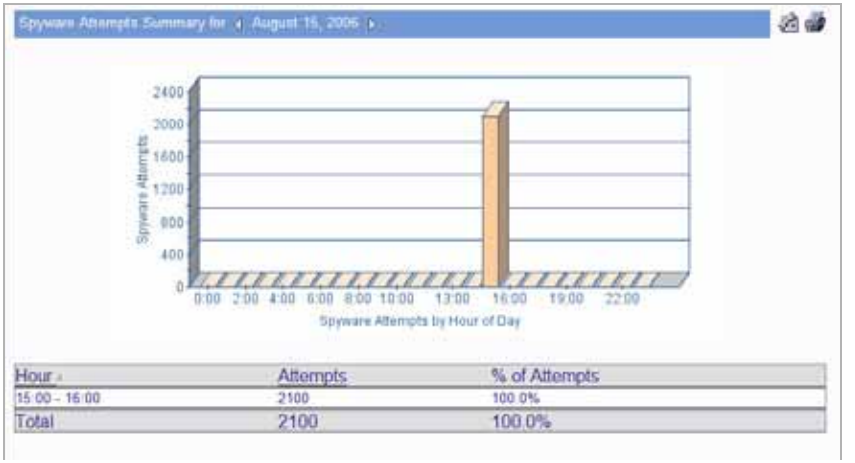
- “Viewing a Spyware Summary” on page 268
- “Viewing Spyware Attempts By Category” on page 269
- “Viewing Spyware Attempts Over Time” on page 270
- “Viewing Spyware Attempts By Category Over Time” on page 272

Viewing a Spyware Summary

The Anti-Spyware Summary report contains information on the number of spyware attempts by hour of the day.

To view a spyware Summary, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of virus attacks attempted during each hour of the day.
5. The table contains the following information:
   - **Hour**—the hour of the day for which the summary is provided.
   - **Attempts**—the number of times the spyware attempted to infect the device during a pre-set time interval (the hour of the day is the default).
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval (the hour of the day is the default).
6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.
9. Note this page displays the number of spyware attempts that occurred during two-hour intervals during the past day.

Viewing Spyware Attempts By Category

These reports display the spyware activity by category including the actual category or classification of the spyware, the priority, and the event/attacks type. By using the category as criteria, you can display details about the type/message text and number of events.

To view spyware attempts by category, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **By Category**. The By Category page displays.

4. The pie chart displays the percentage of spyware attempts by category.
5. The table contains the following information:
   - **Category**—the category of the spyware.
   - **Attempts**—the number of times the spyware attempted to infect the device using the category as a criteria.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts using the category as a criteria.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Spyware Attempts Over Time

You can display spyware attempts over a set time interval. These reports are available at the unit and global levels similar to the other summary reports. To view spyware attempts using pre-set time intervals as the viewing criteria, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Anti-Spyware** tree and click **Over Time**. The Over Time page displays.

4. The bar graph displays the number of spyware attempts that were made during each day over a specified time period.
5. The table contains the following information:
   - **Date**—the date for which the summary is provided.
   - **Attempts**—the number of times the spyware attempted to infect the device during a specific date.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

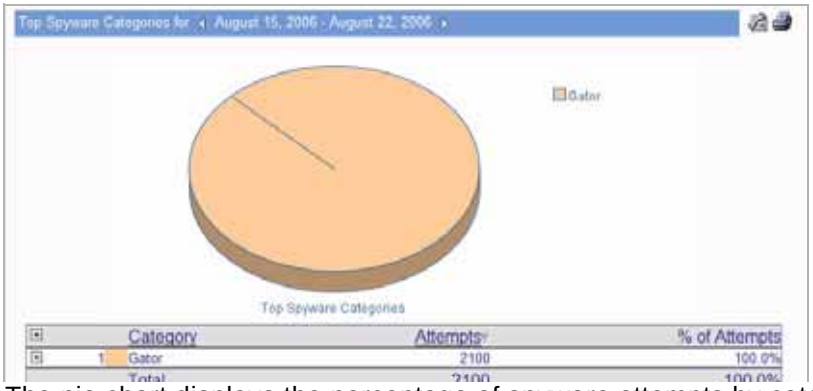
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Spyware Attempts By Category Over Time

You can generate reports that display the spyware activity by category, such as the category, priority, and events/attacks over time. Using the category over time statistic as criteria for report generation provides details about the type/message text and number of events.

To view Anti-Spyware attempts using categories over time intervals as the viewing criteria, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **By Category Over Time**. The By Category Over Time page displays.



4. The pie chart displays the percentage of spyware attempts by category. The table contains the following information:
   - **Category**—the category of the virus.
   - **Attempts**—the number of times the spyware attempted to infect the device during a pre-set time interval.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. To display a limited group of items, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith or john42.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

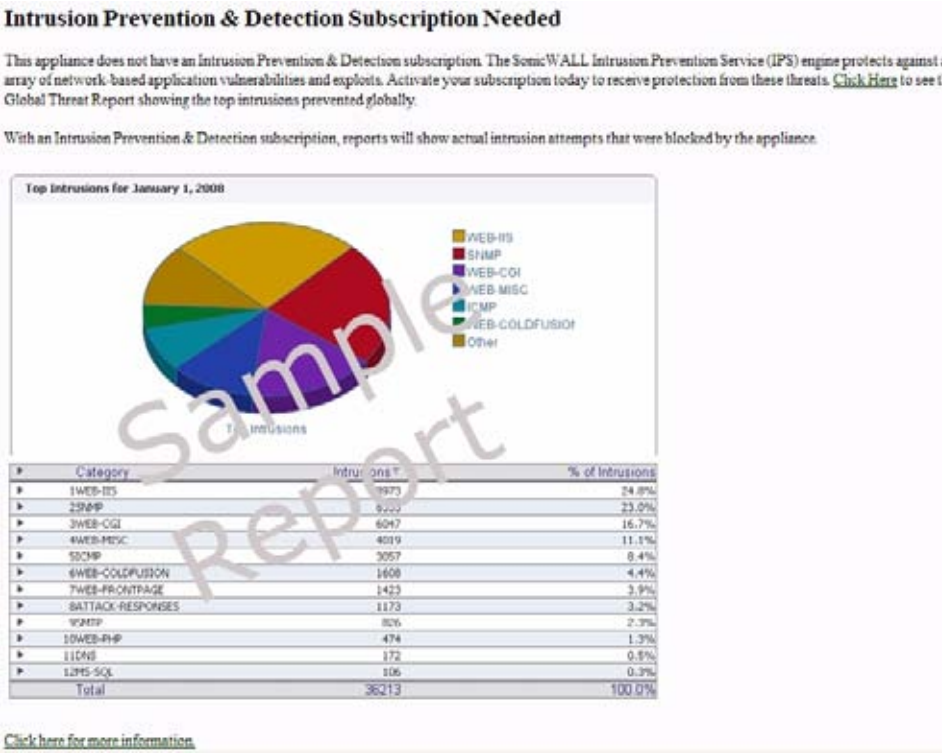
Viewing Intrusion Prevention Reports

The Intrusion Prevention Service (IPS) reports show the number of attempted intrusions that occurred during the specified time period.

Note All reports appear in the appliance’s time zone.

If the selected appliance is not licensed for SonicWALL Intrusion Prevention Service, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all

intrusions and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Intrusion Prevention Service and other subscription services.



Select from the following intrusion reports:

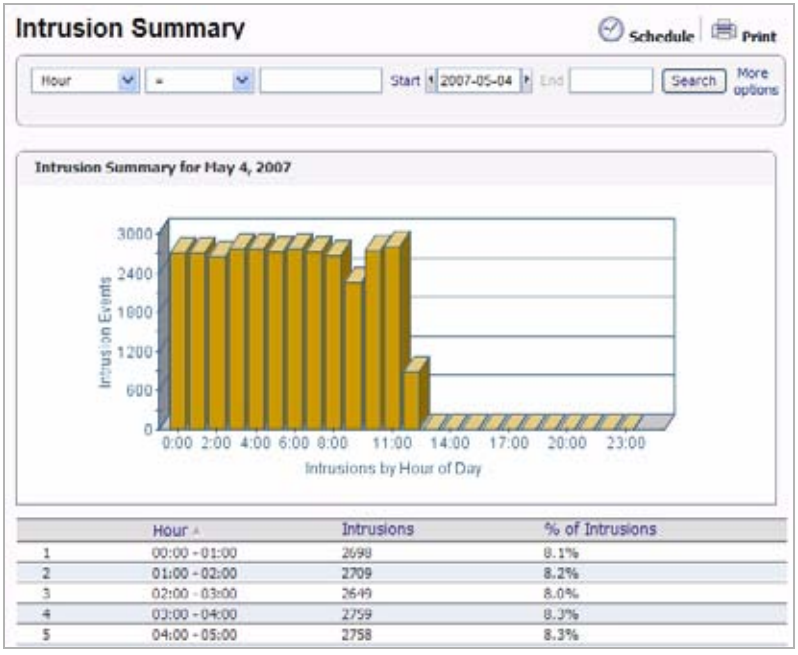
- To view a summary of the attacks, see “Viewing the Intrusion Prevention Summary Report” on page 275.
- To view the attacks by source IP address, see “Viewing the Errors Report” on page 254.
- To view a summary of the errors and exceptions, see “Viewing the Errors Report” on page 254.
- To view attacks over a period of time, see “Viewing Attack Reports Over Time” on page 256.
- To view errors and exceptions over a period of time, see “Viewing Errors Over Time” on page 258.

Viewing the Intrusion Prevention Summary Report

The Attack Summary report contains information on the number of attempted intrusions on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the IPS Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Intrusion Prevention** tree and click **Summary**. The Summary page displays.



	Hour	Intrusions	% of Intrusions
1	00:00 - 01:00	2698	8.1%
2	01:00 - 02:00	2709	8.2%
3	02:00 - 03:00	2649	8.0%
4	03:00 - 04:00	2759	8.3%
5	04:00 - 05:00	2758	8.3%

4. The bar graph displays the number of intrusions attempted during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts on this day, compared to the time period. For example, if 10,000 intrusion attempts occurred during the time period and 1,000 intrusion attempts occurred on Thursday, its **% of Intrusions** field will display 10%.

6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

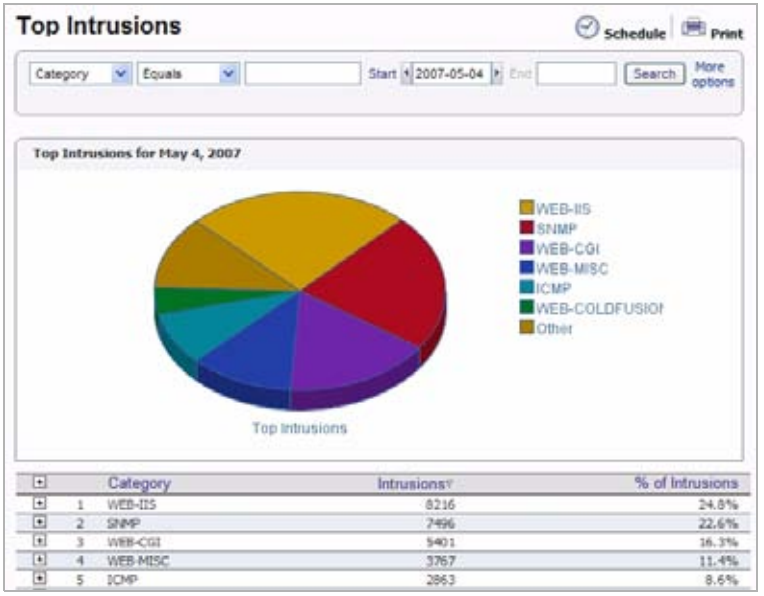
Viewing Intrusion Attempts By Category

These reports display the intrusion activity by category including the actual category or classification of the intrusion, the priority, and the event/attacks type. By using the category as criteria, you can display details about the type/message text and number of events.

To view intrusion attempts by category, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Intrusion Prevention** tree and click **By Category**. The By Category page displays.



4. The pie chart displays a list of intrusions attempted by category. The table contains the following information:
   - **Category**—the category of the intrusion attempt.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts as a portion of the aggregate number of intrusion attempts using the category as a criteria.
5. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

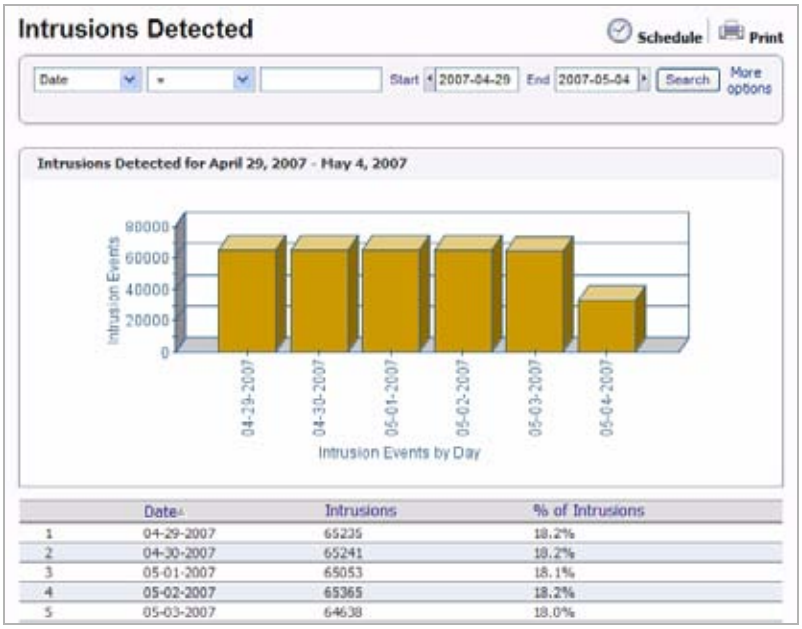
Viewing Intrusions Over Time

The Over Time report displays the daily number of intrusion attempts during the specified time period.

To view the Intrusions Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.

3. Expand the **Intrusion Prevention** tree and click **Intrusions Over Time**. The Intrusions Over Time page displays.



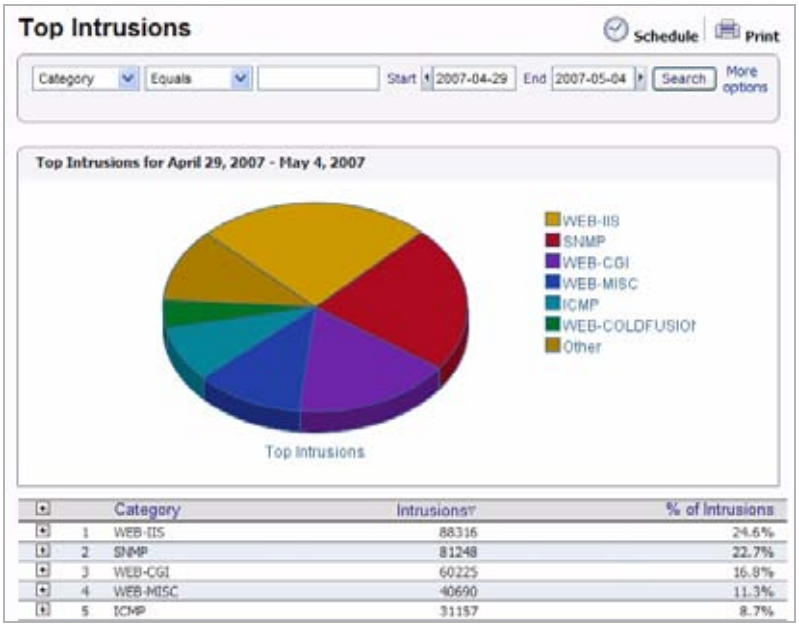
4. The bar graph displays the number of intrusions attempted each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts on this day, compared to the time period. For example, if 10,000 intrusion attempts occurred during the time period and 1,000 intrusion attempts occurred on Thursday, its **% of Intrusions** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Intrusion Reports By Category Over Time

You can generate reports that display the intrusion activity by category, such as the category, priority, and events/attacks over time. Using the category over time statistic as criteria for report generation provides details about the type/message text and number of events. To view intrusion attempts using categories over time intervals as the viewing criteria, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Intrusion Prevention** tree and click **By Category Over Time**. The By Category Over Time page displays.



4. The pie chart displays a list of intrusions attempted by category over time. The table contains the following information:
   - **Category**—the category of the intrusion attempt.
   - **Intrusions**—the number of attempted intrusions during a pre-set time interval.
   - **% of Intrusions**—the percentage of intrusion attempts the current intrusion entry comprises as a portion of the aggregate number of intrusion attempts on the device during a pre-set time interval.

5. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Application Firewall Reports

Application Firewall reports provide information on the applications, users, and Application Firewall policies that are handled by Application Firewall on the selected SonicWALL appliance(s). The Application Firewall feature is available on SonicWALL NSA and SonicWALL TZ 210 Series appliances in SonicOS Enhanced 5.0 and higher.

Application Firewall reports can be used to view Application Firewall usage by the day or over a period of days. Additionally, you can view the top applications, top users, or top policies for Application Firewall on a single SonicWALL NSA or SonicWALL TZ 210 series appliance.

Clickable reports (Graphs and Data) are supported, providing drill-down reporting information by clicking the graphical elements (such as pie chart slices) and data rows. For example, you can drill down to the User report level by clicking a user in one of the Top reports.

Note All reports appear in the appliance's time zone.

Select from the following:

- To view a summary of the daily Application Firewall usage, see "Viewing the Application Firewall Summary Report" on page 282.
- To view Application Firewall usage over time, see "Viewing the Application Firewall Over Time Report" on page 283.

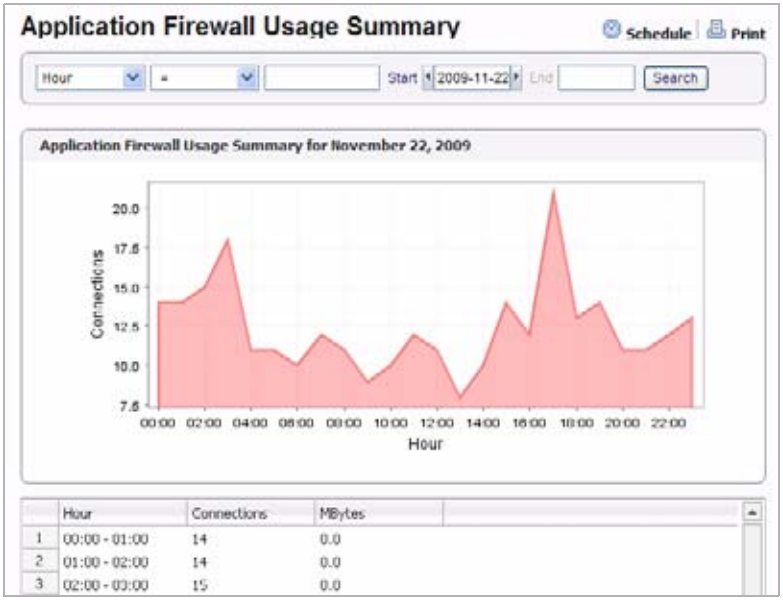
- To view the applications most often intercepted by Application Firewall, see “Viewing Application Firewall Top Applications” on page 284.
- To view the users whose traffic is most often intercepted by Application Firewall, see “Viewing Application Firewall Top Users” on page 285.
- To view the Application Firewall policies that are used the most, see “Viewing Application Firewall Top Policies” on page 286.

Viewing the Application Firewall Summary Report

The Application Firewall Summary report contains information on the number of connections incurring Application Firewall activity logged by a SonicWALL appliance during each hour of the specified day, or at the global level, for all SonicWALL appliances for the day.

To view the Application Firewall Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Summary**. The Summary page displays.



4. The table contains the following information:
   - **Hour**—when the sample was taken

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections

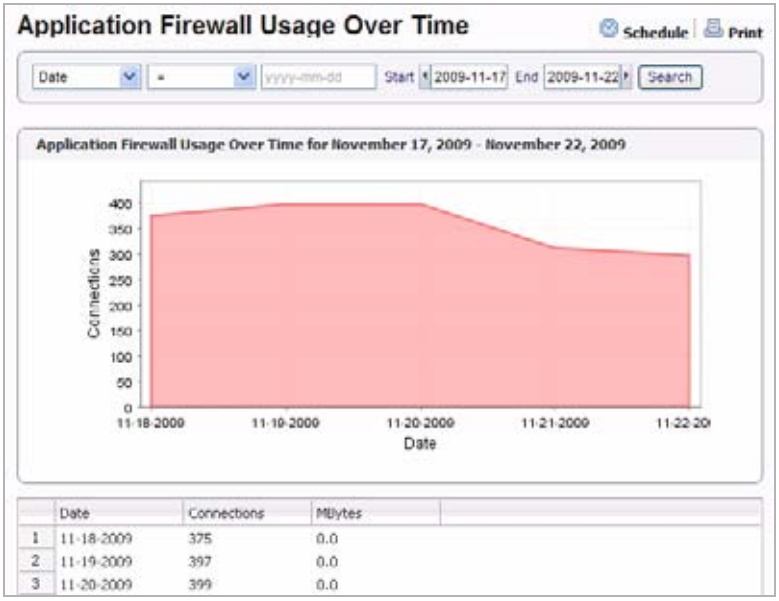
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, click the **Start** and **End** fields to access the drop-down calendars, select the desired dates, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected day or date range.

Viewing the Application Firewall Over Time Report

The Application Firewall Over Time report displays the amount of Application Firewall usage handled by a SonicWALL appliance or a group of SonicWALL appliances for the specified time period.

To view the Application Firewall Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Over Time**. The Over Time page displays.



4. The table contains the following information:
   - **Date**—when the sample was taken

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections

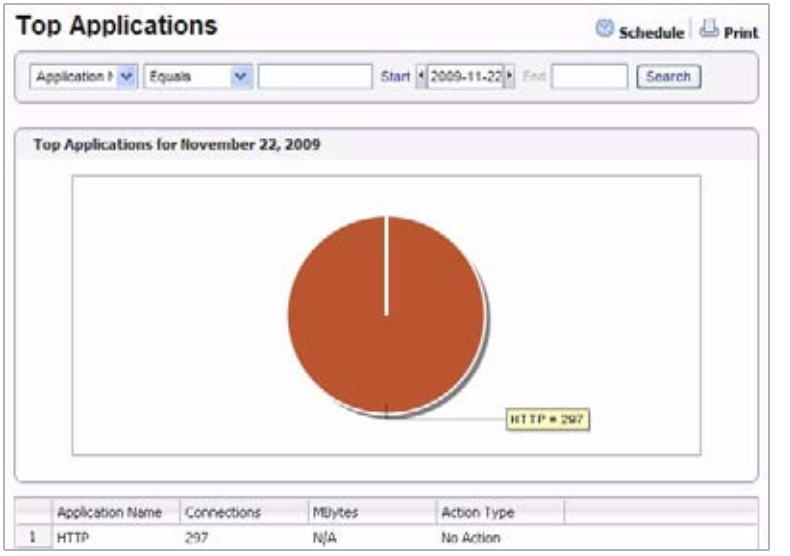
5. To change the date of the report, click the **Start** and **End** fields to access the drop-down calendars, select the desired dates, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Application Firewall Top Applications

The Top Applications report displays the applications that were most logged and/or blocked by Application Firewall on the specified date. The Top Applications report is available at the unit level.

To view the Top Applications report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Top Applications**. The Top Applications page displays.



4. The table contains the following information:
   - **Application Name**—the type of application, such as HTTP, FTP, and so on

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections
- **Action Type**—either No Action, Logged, or Blocked

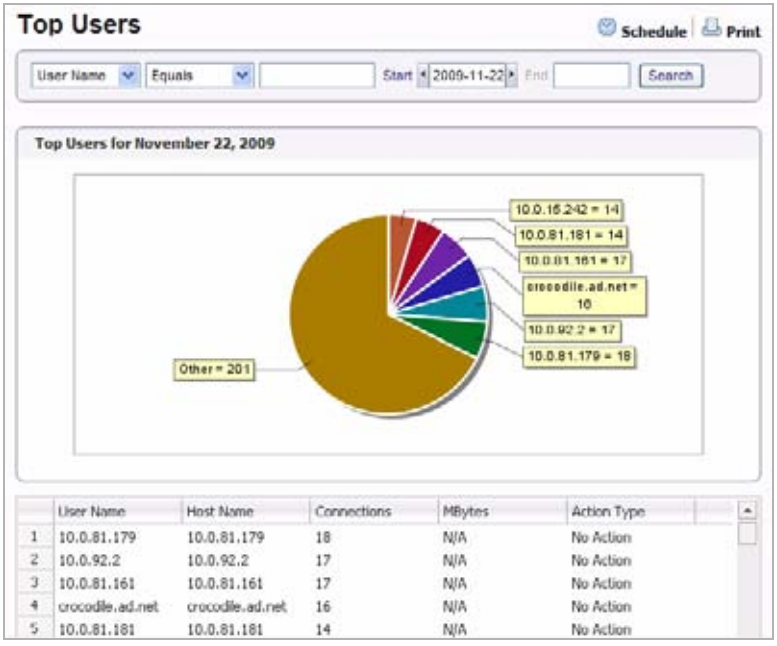
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Application Firewall Top Users

The Top Users report displays the users who made the most logged and/or blocked connections by Application Firewall on the specified date. The Top Users report is available at the unit level.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Top Users**. The Top Users page displays.



4. The table contains the following information:
   - **User Name**—the user's name or IP address
   - **Host Name**—the host name or IP address of the computer that made the connection
   - **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
   - **Mbytes**—megabytes of data transferred during the connections
   - **Action Type**—either No Action, Logged, or Blocked
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

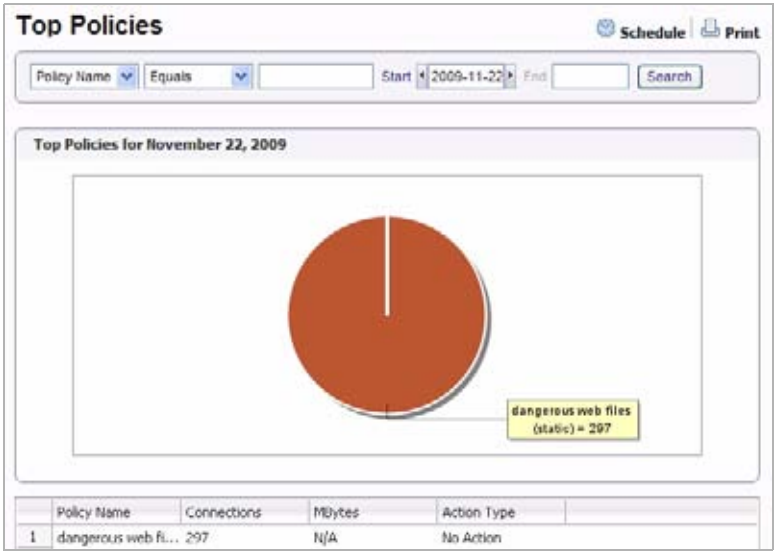
Viewing Application Firewall Top Policies

The Top Policies report displays the Application Firewall policies that were triggered the most on the specified date. The Top Policies report is available at the unit level.

To view the Top Policies report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Application Firewall** tree and click **Top Policies**. The Top Policies page displays.



4. The table contains the following information:
   - **Policy Name**—the Application Firewall policy name
   - **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
   - **Mbytes**—megabytes of data transferred during the connections
   - **Action Type**—either No Action, Logged, or Blocked
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Authentication Reports

The login reports show user logins, administrator logins, and failed login attempts for users and administrators. Authentication reports are available at the unit level.

Note All reports appear in the appliance's time zone.

Select from the following:

- "Viewing the User Login Report" on page 288
- "Viewing the Administrator Login Report" on page 289
- "Viewing the Failed Login Report" on page 289

Viewing the User Login Report

The user login report shows users that logged on to the SonicWALL appliance during the specified day to bypass content filtering or to remotely access local network resources.

To view the User Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Authentication** tree and click **User Login**. The User Login page displays.

User Logins for: August 15, 2006
Displaying records 1–1 of 1 Prev 1 Next 1
Time
Source
* Report produced for timezone: Pacific Time (US & Canada)
* Reports generated based on data summarized on: 08/15/2006 10:16:52 UTC
* Reports generated for the following settings: (User: admin)
Chart Type=BAR PIE, Display Type=Chart & Table, Top Sites=All, Top Users=All, Sites Per User=100, Items=All,
Entries Per Item=100, Site Filter=None, User Filter=None, Whole IP Search Enabled=No, Hours=0 To 23
* Report generated in: 0.031 secs

4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

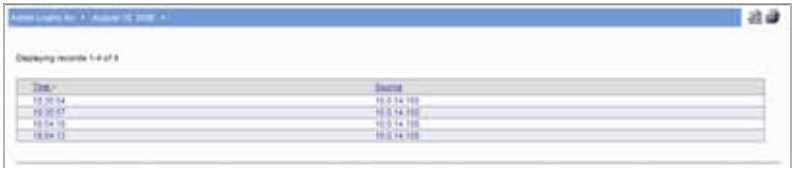
   See "Managing Report Settings" on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Administrator Login Report

The administrator login report shows successful administrator logins during the specified day. This report is useful for identifying misuse and unauthorized management of a SonicWALL appliance.

To view the Admin Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Authentication** tree and click **Admin Login**. The Admin Login page displays.



4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

   See “Managing Report Settings” on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Failed Login Report

The failed login report shows failed login attempts for users and administrators that attempted to log on to the SonicWALL appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Authentication** tree and click **Failed Login**. The page displays.

4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
   - **IP Address**—IP address of the user.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

   See "Managing Report Settings" on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Log

The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance. This information is stored for the time that you specified in the configuration settings.

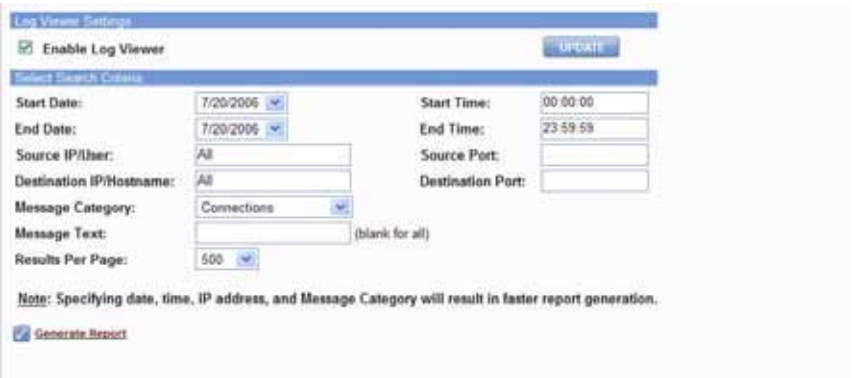
It is necessary to enable the Log Viewer for UTM or SSL-VPN appliances for which you wish to generate Custom Reports. See "Using Custom Reports on UTM Appliances" on page 163.

Note The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For more information, see "Scheduling and Configuring Reports" on page 133.

Viewing the Log for a SonicWALL Appliance

To view the Log, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Log Viewer** tree and click **Search**. The Search page displays.

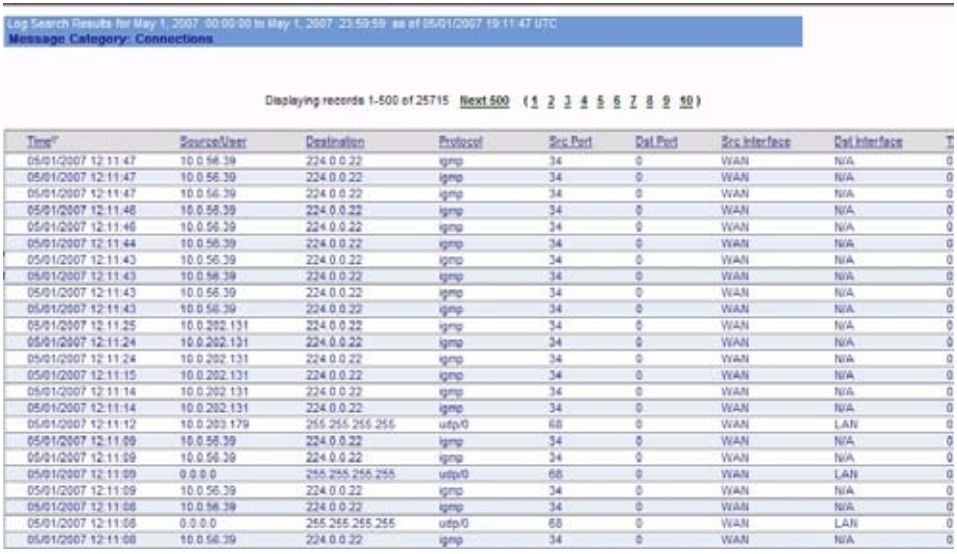


4. Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer. The maximum number of appliances for which Log Viewer can be enabled is controlled on the Console > Reports > Settings page. See "Controlling the Number of Appliances with Log Viewer Enabled" on page 72.

Note Custom Reports are available on appliances with Log Viewer enabled. See "Using Custom Reports on UTM Appliances" on page 163.

5. Under Select Search Criteria, select the date range to view data from in the **Start Date** and **End Date** fields.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.
8. To limit the report to data originating from specific IP addresses or users, enter the source IP address or user name in the **Source IP/User** field. To view all IP addresses, enter **All**.
9. To view log entries for data originating from a particular port, enter the port number in the **Source Port** field.

10. To limit the report to data going to specific IP addresses or hosts, enter the destination IP address or host name in the **Destination IP/Hostname** field. To view log entries for data going to all IP addresses, enter **All**.
11. To view log entries for data going to a particular port, enter the port number in the **Destination Port** field.
12. Select the type of events to view from the **Message Category** list box.
13. To limit the report to messages containing a specific text string, enter the text in the **Message Text** field. Leave the field blank to view all messages.
14. Select the number of entries to display per page from the **Results Per Page** field.
15. Click **Generate Report**. The Log Viewer Results page displays.


Log Search Results for May 1, 2007 00:00:00 to May 1, 2007 23:59:59 as of 05/01/2007 19:11:47 UTC
Message Category: Connections

Displaying records 1-500 of 25715 Next 500 (1 2 3 4 5 6 7 8 9 10)

Time	Source/User	Destination	Protocol	Src Port	Dst Port	Src Interface	Dst Interface	T
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:46	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:46	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:44	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:25	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:24	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:24	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:15	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:14	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:14	10.0.202.131	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:12	10.0.203.179	255.255.255.255	udp/0	68	0	WAN	LAN	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:09	0.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:08	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0
05/01/2007 12:11:08	0.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0
05/01/2007 12:11:08	10.0.56.39	224.0.0.22	igmp	34	0	WAN	N/A	0

16. Search through the entries to find the information for which you are searching. To view the next page of entries, click **Next**.
17. To generate another report, click **Search** again in the **Log Viewer** tree.

CHAPTER 16
SSL-VPN Reporting

This chapter describes how to manage SonicWALL ViewPoint SSL-VPN reporting by customizing and defining scheduled reports and summarization for SSL-VPN appliances.

For details about viewing specific SSL-VPN reports, see “Viewing SSL-VPN Reports” on page 299.

This chapter contains the following sections:

- “SSL-VPN Reporting Overview” section on page 293
- “Using and Configuring SSL-VPN Reporting” section on page 295

SSL-VPN Reporting Overview

This section provides an introduction to the SSL-VPN reporting feature. This section contains the following subsections:

- “What is SSL-VPN Reporting?” section on page 294
- “Benefits of SSL-VPN Reporting” section on page 294
- “How Does SSL-VPN Reporting Work?” section on page 295

After reading the ViewPoint SSL-VPN Reporting Overview section, you will understand the main steps to be taken in order to create and customize reports successfully.

What is SSL-VPN Reporting?

SSL-VPN reporting allows you to configure and design the way you view your reports and the manner in which you receive them. This feature offers various types of static and dynamic reporting in which you can customize the way information is reported.

SonicWALL ViewPoint SSL-VPN reporting provides a visual presentation of all your configured report settings and information. With SSL-VPN reporting, you are able to view your reports in new enhanced graphs, create granular, custom reports, create scheduled reports, and search for reports using the search bar tool.

Custom reports are also available in SSL-VPN reporting. SonicWALL SSL-VPN appliances provide a Resource Activity custom report for tracking the source, destination, and other information about resource activity passing through a SonicWALL SSL-VPN device.

The Custom Reports feature provides an intuitive, responsive interface for customizing the report layout and configuring content filtering prior to generating the report. Two types of reports are available: Detailed Reports and Summary Reports. Both provide detailed information, but are formatted to meet different needs. A Detailed Report displays the data in sortable, resizable columns, while a Summary Report provides top level information in graphs that you can click to drill down for detailed information.

Once you set up a Custom Report that meets your needs, you can save your settings as a template for reuse, set a schedule to run the report, export the report as a PDF or CSV (Excel) file, or print report pages.

Benefits of SSL-VPN Reporting

SSL-VPN reports provide visibility into the resource use by logged in users, leading to policies that enhance the user experience and the productivity of employees. The following capabilities contribute to the benefits of the SSL-VPN reporting feature:

- Custom reports can track events to the minute or second of the day for forensics and troubleshooting
- Interactive charts allow drill-down into specific details
- Table structure with ability to adjust column width of data grid
- Improved report navigation
- Report search
- Scheduled reports

How Does SSL-VPN Reporting Work?

SSL-VPN appliances send syslog data to the ViewPoint syslog collector, similar to SonicWALL UTM appliances. Once summarization takes place, you can create, schedule, view, and search for SSL-VPN reports from the ViewPoint central reporting interface.

SSL-VPN Custom Reports are based on raw syslog information contained in a database that is created daily from the raw syslog data sent from all managed or monitored appliances. This database is saved using a date/time suffix, and contains tables full of data for each appliance. All the syslog data received by SonicWALL ViewPoint is available in the database.

Note The raw syslog database required by Custom Reports is not enabled by default, as it is highly resource intensive. This functionality must be enabled per unit in the UTM > Log Viewer screen.

SSL-VPN Reporting supports scheduled reports to be sent on a daily, weekly, or monthly basis to any specified email address.

Using and Configuring SSL-VPN Reporting

This section describes how to use and configure SSL-VPN reporting. See the following subsections:

- "About Viewing Available SSL-VPN Report Types" section on page 295
- "Configuring SSL-VPN Scheduled Reports" section on page 296

About Viewing Available SSL-VPN Report Types

To view the available types of reports for SSL-VPN, perform the following steps:

1. Log into your ViewPoint management console.
2. Click the **SSL-VPN** tab.

   The SSL-VPN screen displays the following list of reports:

   Node Level reports:

   – **General**

   –Status: information about the appliance

- **Bandwidth**
  - –Summary: total connections listed by hour
  - –Top Users: connections listed by user
  - –Over Time: connections listed by date
  - –Top Users Over Time: connections listed by user for the selected date range
- **Custom Report**
  - –Resource Activity: source, destination, and other information about resource activity
- **Resources**
  - –Summary: connections per connection protocol (HTTPS, NetExtender, etc)
  - –Top Users: connections listed by user
- **Authentication**
  - –User Login: user, time, and source of successful authentication-daily. User Login reports now combine admin users with all other users in the same report.
  - –Failed login: time and source host of failed logins for one day

Global Level Reports:

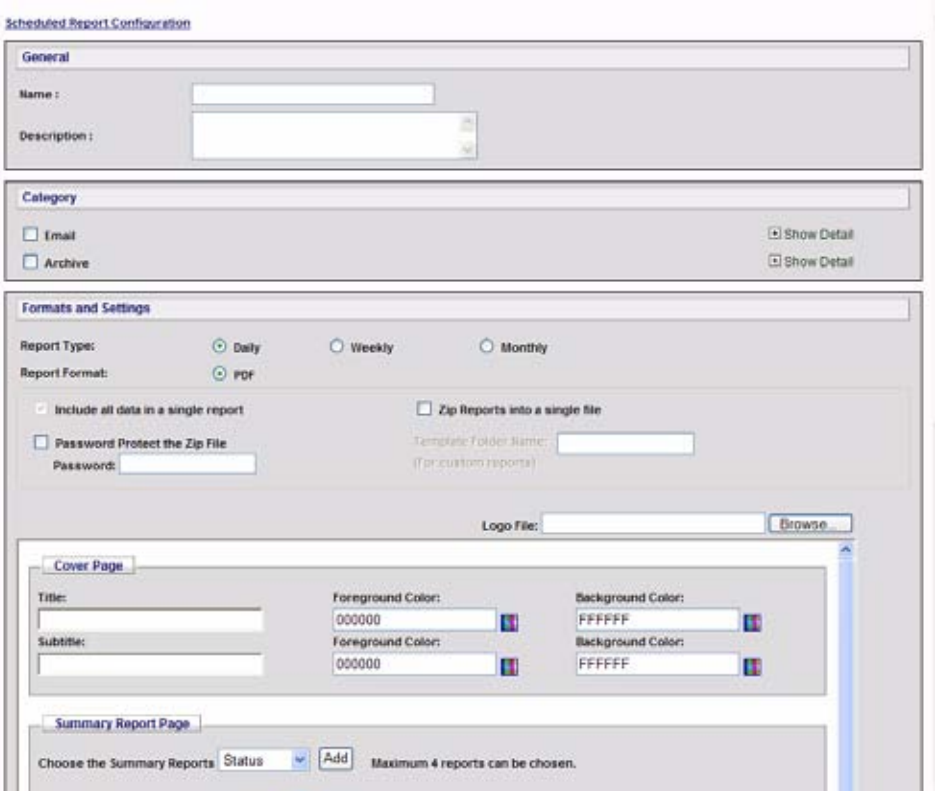
- **General**
  - –Status: number of units in the system and their ViewPoint license status
- **Bandwidth**
  - –Summary: connections per SSL-VPN appliance
  - –Over Time: total connections by date for group

Configuring SSL-VPN Scheduled Reports

To configure SSL-VPN scheduled reports and summarization, perform the following tasks:

1. On the **SSL-VPN** tab, navigate to **Configuration > Scheduled Reports**.
2. Click the **Add** button.

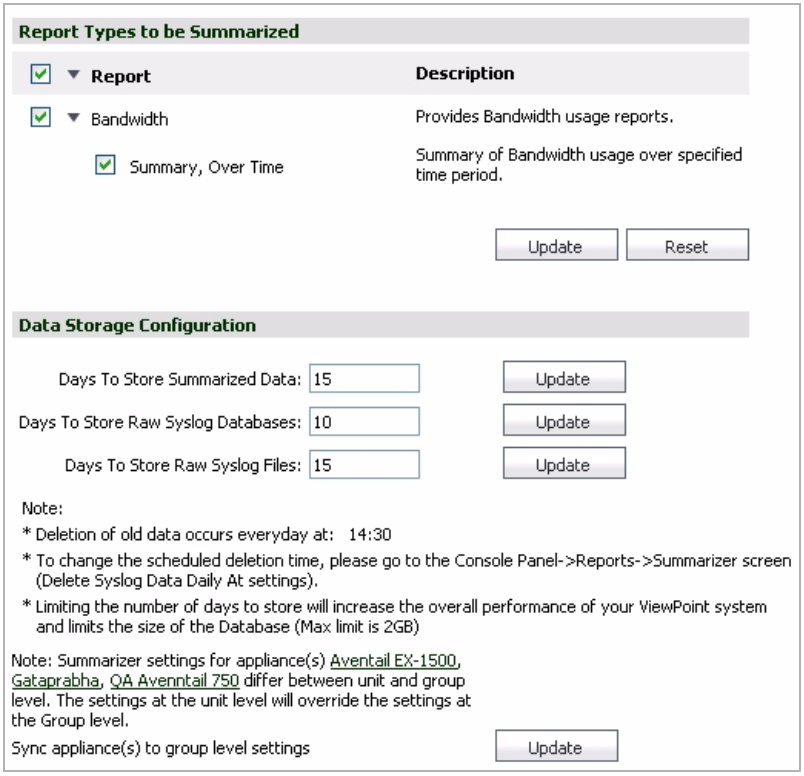
3. The Scheduled Report Configuration form displays. Fill out the fields accordingly. For more information, see the following sections:
   - "Configuring Scheduled Reports" on page 134
   - "Scheduling PDF Compliance Reports" on page 144



Configuring SSL-VPN Summarization

1. On the **SSL-VPN** tab, navigate to **Configuration > Summarizer Settings**. The reports that can be summarized for a SSL-VPN appliance are configurable at either global or unit level. The screen displays the configuration appropriate for the level. The report type lists can also be expanded for a detailed description of report content.

The report types you can summarize are shown below.


Report Types to be Summarized
Report
Description
Bandwidth
Provides Bandwidth usage reports.
Summary, Over Time
Summary of Bandwidth usage over specified time period.
Update
Reset
Data Storage Configuration
Days To Store Summarized Data: 15
Update
Days To Store Raw Syslog Databases: 10
Update
Days To Store Raw Syslog Files: 15
Update
Note:
* Deletion of old data occurs everyday at: 14:30
* To change the scheduled deletion time, please go to the Console Panel->Reports->Summarizer screen (Delete Syslog Data Daily At settings).
* Limiting the number of days to store will increase the overall performance of your ViewPoint system and limits the size of the Database (Max limit is 2GB)
Note: Summarizer settings for appliance(s) Aventail EX-1500, Gataprabha, QA Avenntail 750 differ between unit and group level. The settings at the unit level will override the settings at the Group level.
Sync appliance(s) to group level settings
Update

SSL-VPN reports generated in ViewPoint can be exported in PDF format, providing easy online transfer. For more information about the Summarizer and exporting reports in PDF format, see:

- "Selecting Reports for Summarization" on page 137
- "Configuring Data Storage Settings" on page 139
- "Using Summarize Now" on page 76
- "Scheduling PDF Compliance Reports" on page 144

CHAPTER 17
Viewing SSL-VPN Reports

This chapter describes the available reports for SonicWALL SSL-VPN appliances.

For information on how to configure scheduled reports and summarization, see:

- “Using and Configuring SSL-VPN Reporting” on page 295

Select from the following reports:

- “Viewing General Status Reports” section on page 299
- “Viewing SSL-VPN Bandwidth Reports” section on page 301
- “Using SSL-VPN Custom Reports” section on page 307
- “Viewing SSL-VPN Resources Reports” section on page 325
- “Viewing SSL-VPN Authentication Reports” section on page 330
- “Viewing the SSL-VPN Log” section on page 332

Viewing General Status Reports

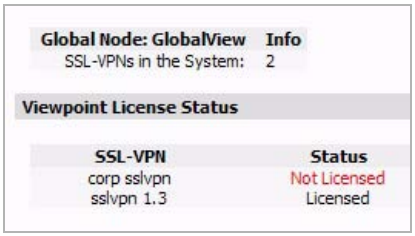
The **General > Status** page contains information about the SSL-VPN appliance or group of SSL-VPN appliances.

To view the Status page, perform the following steps:

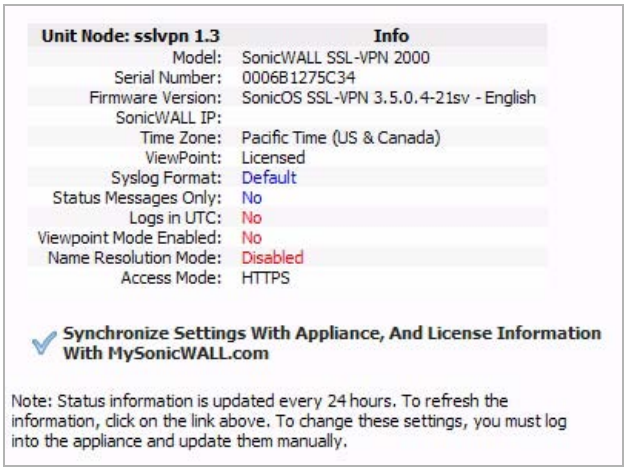
1. Click the **SSL-VPN** tab.
2. Select **MyReportsView** or an SSL-VPN appliance in the left pane.

3. In the center pane, expand the **General** tree and click **Status**. The Status page displays.

   When **MyReportsView** is selected, the Status page displays the license status of all SSL-VPN appliances.



   When a unit is selected, the Status page displays information about the SSL-VPN appliance, including model, serial number, firmware version, time zone, license status, log settings, and other settings.


Unit Node: sslvpn 1.3
Info
Model: SonicWALL SSL-VPN 2000
Serial Number: 0006B1275C34
Firmware Version: SonicOS SSL-VPN 3.5.0.4-21sv - English
SonicWALL IP:
Time Zone: Pacific Time (US & Canada)
ViewPoint: Licensed
Syslog Format: Default
Status Messages Only: No
Logs in UTC: No
Viewpoint Mode Enabled: No
Name Resolution Mode: Disabled
Access Mode: HTTPS
Synchronize Settings With Appliance, And License Information With MySonicWALL.com
Note: Status information is updated every 24 hours. To refresh the information, click on the link above. To change these settings, you must log into the appliance and update them manually.

4. In the unit view, to synchronize settings with the SSL-VPN appliance and license information with MySonicWALL, click **SynchronizeSettings With Appliance, And License Information With Mysonicwall.com**.

Viewing SSL-VPN Bandwidth Reports

Bandwidth reports display the amount of data transferred through one or more selected SSL-VPN appliances.

Bandwidth reports are an ideal starting point for viewing overall bandwidth usage. You can view bandwidth usage view by hour, day, or over a period of days. Additionally, you can view the top users of bandwidth.

From this information, you can determine network strategies. For example, if you need more bandwidth, you might need to upgrade network equipment, or you might simply need to curtail the bandwidth usage of a few employees.

Note All reports appear in the time zone of the selected appliance.

Select from the following:

- “Viewing SSL-VPN Bandwidth Summary Reports” on page 301
- “Viewing SSL-VPN Top Users of Bandwidth Reports” on page 303
- “Viewing SSL-VPN Bandwidth Usage Over Time Reports” on page 304
- “Viewing SSL-VPN Top Users of Bandwidth Over Time Reports” on page 306

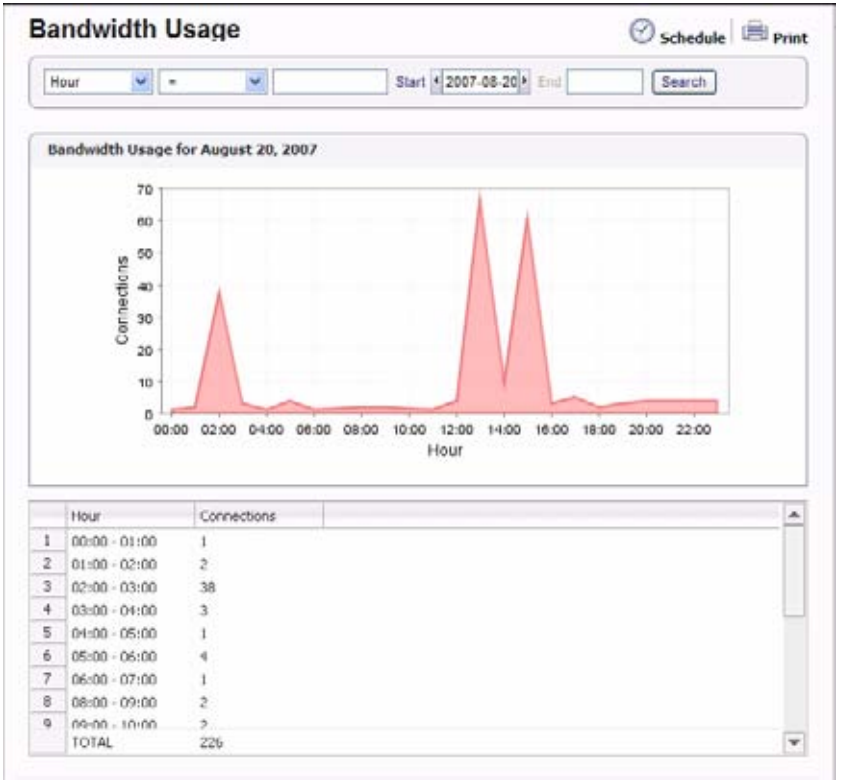
Viewing SSL-VPN Bandwidth Summary Reports

The Bandwidth Summary report shows the number of connections handled by a SSL-VPN appliance during each hour of the specified day, or at the global level, by each SSL-VPN appliance for the day.

To view the Bandwidth Summary report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select the global icon or a SSL-VPN appliance.

3. Expand the **Bandwidth** tree and click **Summary**. The Summary page displays.



4. The graph displays the number of connections to the SSL-VPN appliance during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Connections**—number of connections to the SSL-VPN appliance
6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, click the **Start** field to access the drop-down calendar.
7. After selecting a date, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

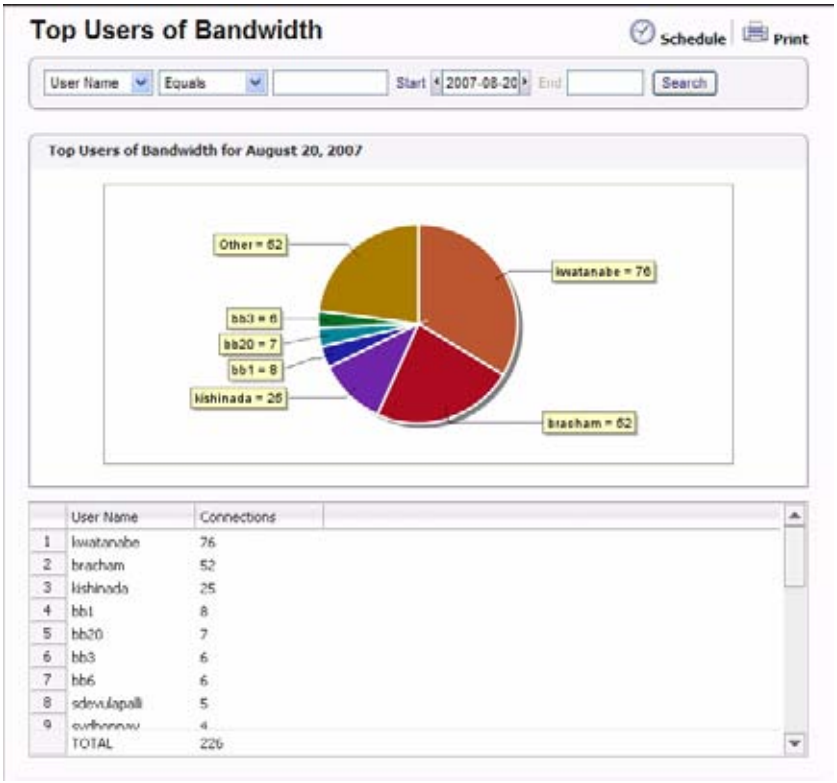
Note The date setting will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Top Users of Bandwidth Reports

The Top Users report displays the users who used the most connections on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Bandwidth** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of connections used by each user.

5. The table contains the following information for all users:
   - **Users**—the user name
   - **Connections**—number of connection events or “hits”
6. By default, the ViewPoint Reporting Module shows yesterday’s report, a pie chart for the top six users, and a table for all users. To change the date of the report, click the **Start** field to access the drop-down calendar.
7. To display a limited number of users, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note The date setting will stay in effect for all similar reports during your active login session.

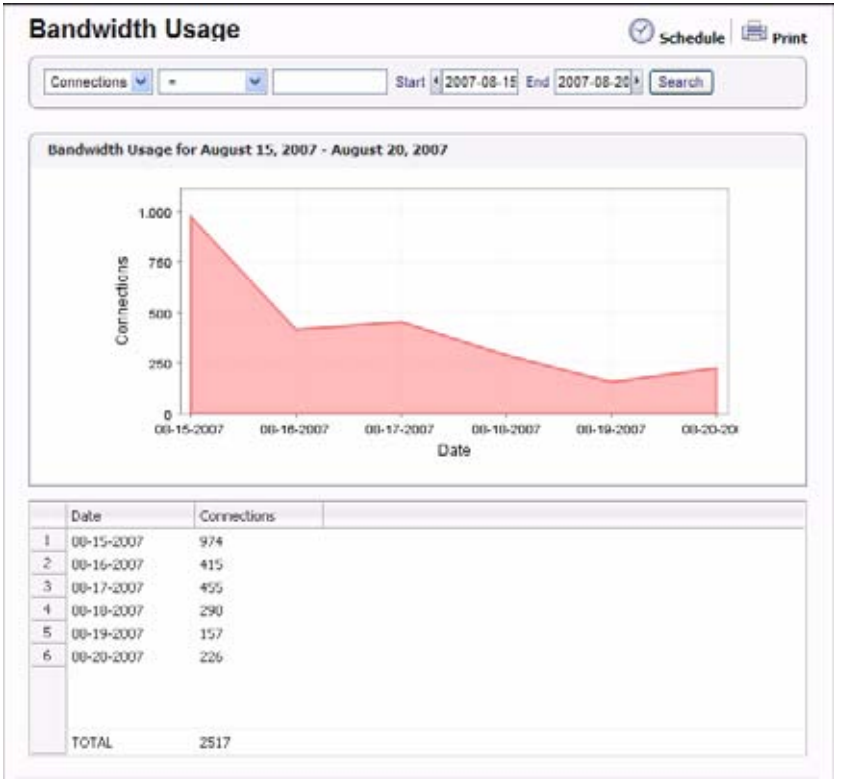
Viewing SSL-VPN Bandwidth Usage Over Time Reports

The Bandwidth Usage Over Time report displays the daily number of connections handled by a SSL-VPN appliance or a group of SSL-VPN appliances for the specified time period.

To view the Bandwidth Usage Over Time report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select the global icon or a SSL-VPN appliance.

3. Expand the **Bandwidth** tree and click **Over Time**. The Over Time page displays.



4. The graph displays the number of connections during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken
   - **Connections**—number of hits
6. To change the date of the report, use the Search Bar and click the **Start** or **End** fields to access the drop-down calendar.
7. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date range.

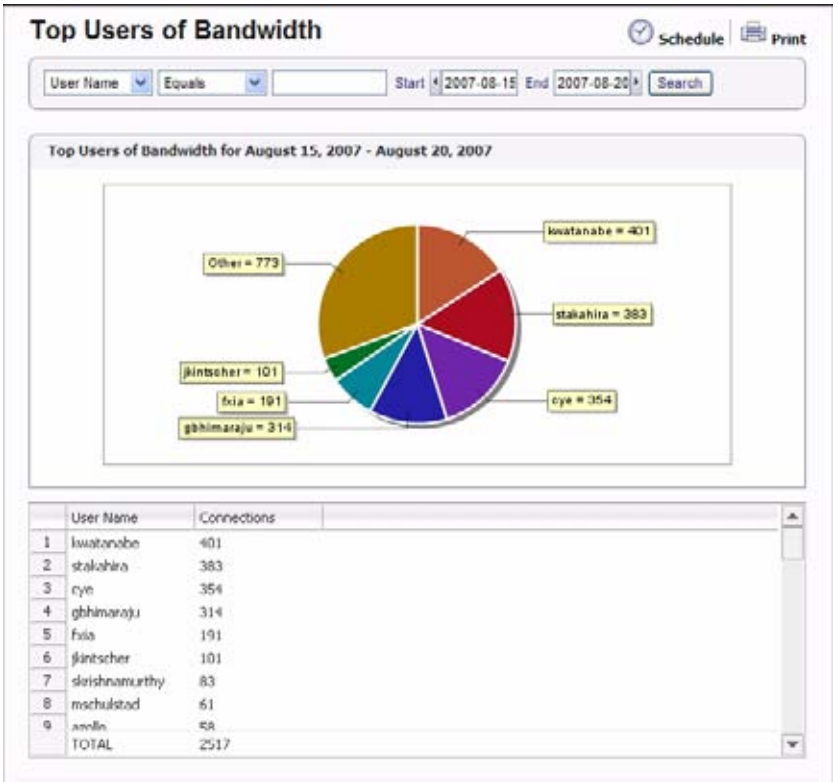
Note These date settings will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Top Users of Bandwidth Over Time Reports

The Top Users Over Time report displays the users who used the most connections during the specified date range. This report is available at the unit level.

To view the Top Users Over Time report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Bandwidth** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the percentage of connections used by the top users.

5. The table contains the following information for all users:
   - **Users**—the user name of the user
   - **Connections**—number of connection events or “hits”
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, click the **Start** or **End** field to access the drop-down calendar.
7. To display a limited group of users, enter the user IDs in the **Search Bar** fields.

Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

8. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected users and date range.

Note These settings will stay in effect for all similar reports during your active login session.

Using SSL-VPN Custom Reports

Custom Reports are available at the unit level for appliances visible on the SSL-VPN tab. Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see “Viewing the SSL-VPN Log” on page 332.

When configuring a Custom Report on the Resource Activity page, the Template Section acts as a query builder. You select the criteria for the report that you want, and SonicWALL ViewPoint uses your input to query the raw syslog database for the information, and then outputs the report. The Template Section consists of two parts: the Date/Time section and the Report Layout section.

After building your query in the Template Section and clicking the **Generate Report** button, the report is displayed in the Report Section. The Report Section is displayed in the lower half of the page, under the Template Section; this layout is called Split Mode. You can easily toggle between Split Mode and Full Mode. Full Mode can be used to display only the Template Section or only the Report Section in a full page view.

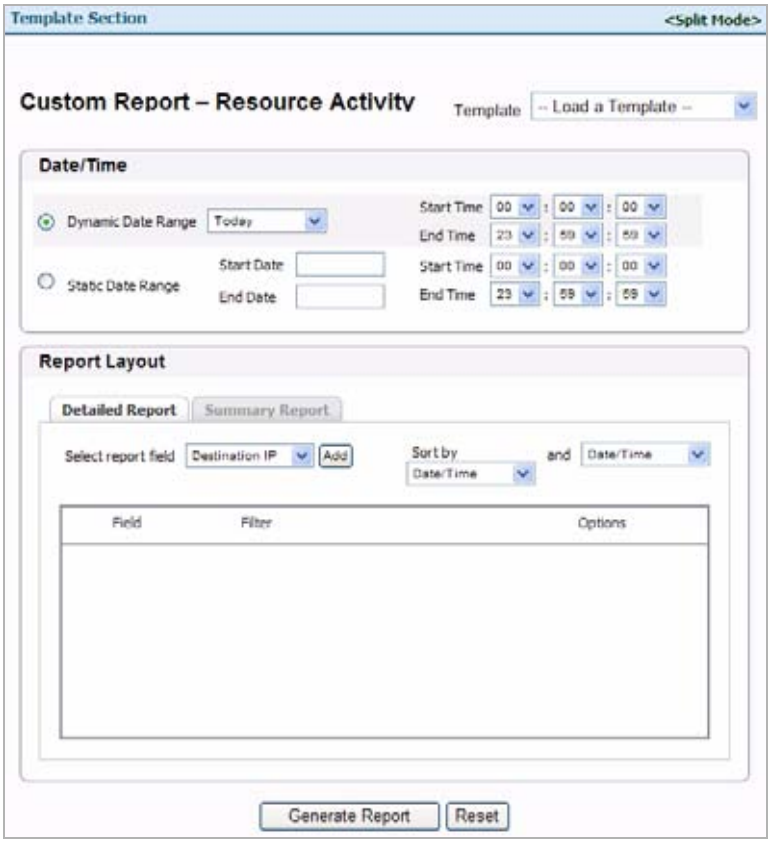
The Report Section displays the report and provides controls for pagination, printing, and exporting the report in PDF or CSV format. You can also click the **Save Template** button in this section if you want to save the settings for this report as a template for reuse later. See the following sections for detailed information:

- "Toggling Between Split Mode and Full Mode" on page 308
- "Configuring the Date and Time for Custom Reports" on page 311
- "Configuring the Report Layout and Generating the Report" on page 314
- "Generating the Custom Report" on page 320
- "Viewing a Custom Report" on page 321
- "Printing a Page or Exporting the Report as a PDF or CSV File" on page 323
- "Saving the Report Template" on page 324

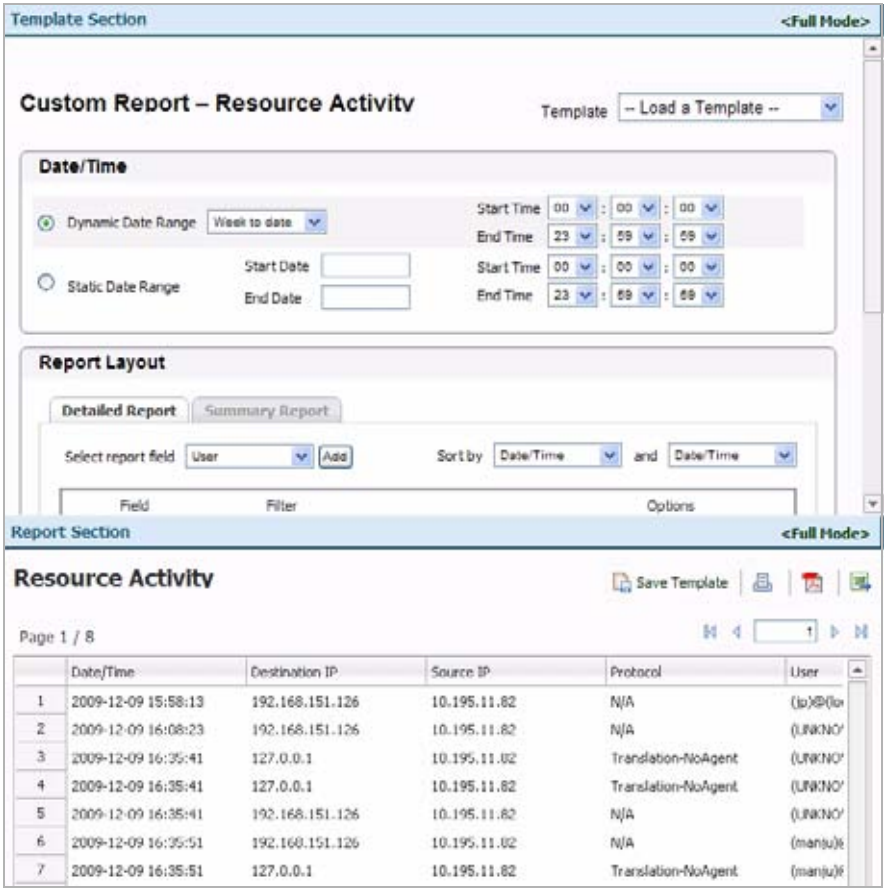
Toggling Between Split Mode and Full Mode

The Custom Report page contains two main sections, the Template Section and Report Section, which can be displayed together or independently depending on the mode.

When the Custom Report page is initially displayed for a selected appliance, the Template Section is displayed in Full Mode. Split Mode is available, but the Report Section displays no data until a report has been generated. The image below shows the Custom Report > Resource Activity page with the Template Section displayed in Full Mode.



After generating a report, the page automatically changes to Split Mode and displays the report settings in the Template Section in the top half of the page and the report results in the Report Section in the lower portion. The image below shows the Template Section and Report Section displayed in Split Mode.



At any time, you can change to Full Mode if you want to display either the Template Section or the Report Section individually. From Full Mode, you can easily change back to Split Mode.

To toggle between Split Mode and Full Mode:

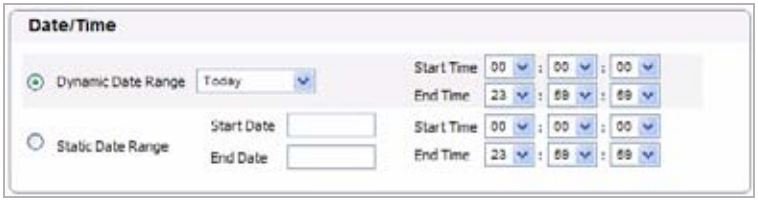
1. Select a unit for which Log Viewer is enabled, and then navigate to the **Custom Report** page.
2. On a page that is currently displayed in Full Mode, to change the view to Split Mode click the **<Split Mode>** button at the right side of the section heading.

3. On a page that is currently displayed in Split Mode, do one of the following to change to a Full Mode display of either the Template Section or the Report Section:
   - Click the **<Full Mode>** button to the right of the Template Section heading.
   - Click the **<Full Mode>** button to the right of the Report Section heading.

Configuring the Date and Time for Custom Reports

At the top of the Template Section of the Custom Report page, the Date/Time region provides a way to designate the time period to use when generating the report. You can select either a Dynamic Date Range or a Static Date Range.

Both the Dynamic Date Range and the Static Date Range provide Start Time and End Time settings. By using the Start Time and End Time fields, you can specify the exact hour, minute, and second for both the beginning and the end of the period for the report. When a start and end time is specified for a date range containing multiple days, the start/end times are applied to each day of the period when analyzing data for the report. The default is to include data for the full 24 hours in each day of the date range.



Dynamic Date Range

The **Dynamic Date Range** selection allows you to select from four date ranges and to specify the exact starting and ending times on the days in the selected date range for the log data to be used for the report.

For the **Dynamic Date Range**, you can select from the following four date choices:

- **Today** – Uses log data from the current date, beginning just after midnight
- **Yesterday** – Uses log data from just after midnight of the previous day, up to and including the most recent log message from the current date

- **Week to Date** – Uses log data from the current date, plus the seven preceding days
- **Month to Date** – Uses log data from the same date as the current date in the previous month, up to and including the most recent log message from the current date

When generating a report with a template containing a dynamic date range setting, the dates used when referencing the log data are relative to the current date. Thus, two reports generated from the same template on different days will provide different results.

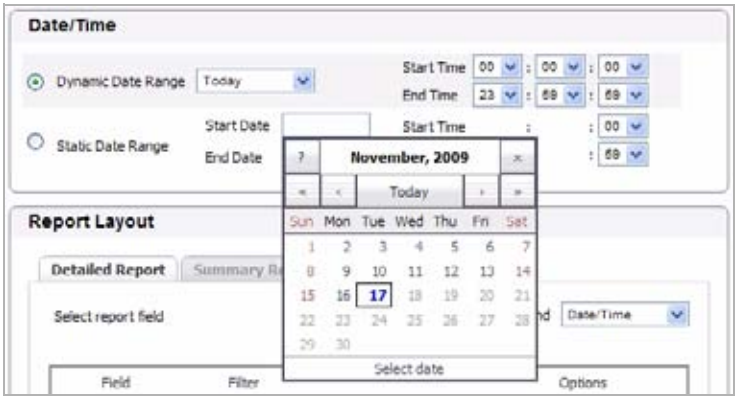
To select a Dynamic Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Dynamic Date Range** radio button.
3. In the drop-down list, select **Today**, **Yesterday**, **Week to Date**, or **Month to Date**.
4. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Dynamic Date Range row. These settings specify the earliest data to be included in the report, for each day of the date range.
5. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data to be included in the report, for each day of the date range.
6. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Static Date Range

The **Static Date Range** selection allows you to specify the exact dates, starting, and ending times on the days in the selected date range for the log data to be used for the report. You can specify a single date or a date range, and indicate the exact hour, minute, and second for both the beginning and the end of the daily period for the report.

A popup calendar makes it easy to select the Start Date and End Date for the date range, as shown below.



To specify a Static Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Static Date Range** radio button.
3. Click the **Start Date** field to access the pop-up calendar.
4. Use the navigation arrows near the top of the calendar to change the year or month. Click the **<<** button to move to the previous year, or hold the button to select from a list of years. Click the **>>** button to move to the next year, or hold the button to select from a list of years. Similarly, click the **<** or **>** to move back or ahead by one month, or hold the button to select from a list of months.
5. Click the desired start date in the calendar. This adds the date to the **Start Date** field and closes the calendar.
6. Click the **End Date** field to access the pop-up calendar.
7. Use the navigation arrows near the top of the calendar to change the year or month.
8. Click the desired end date in the calendar. This adds the date to the **End Date** field and closes the calendar.
9. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Static Date Range row. These settings specify the earliest data for each day in the date range to be included in the report.

10. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data for each day in the date range to be included in the report.
11. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Configuring the Report Layout and Generating the Report

Located in the Template Section of the Custom Report page below the Date/Time region, the Report Layout region provides a way to specify the type of data to include, and the format of the report. The Report Layout region has a Detailed Report tab and a Summary Report tab. The report appearance and the way information is organized is quite different between a Detailed Report and a Summary Report.

The Detailed Report tab contains a list of data categories that you can add as report fields, and allows you to specify query values for each. The categories you select will appear as column headings in the report.

The Summary Report tab allows you to structure a report showing the top elements of Resource Activity. You can select the number of top elements, what to base the comparisons on, and the two data categories to evaluate when determining the top elements. The generated report provides graphical output that you can click to drill down for detailed information.

For more information about each of these Report Layout tabs, see the following sections:

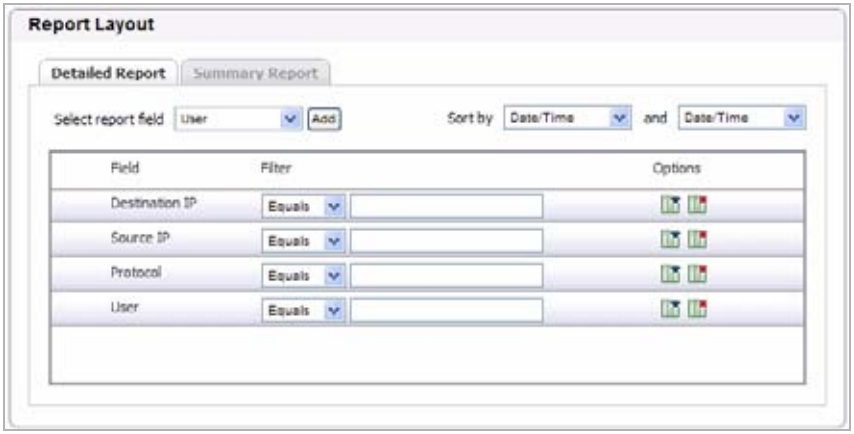
- “Detailed Reports” on page 315
- “Summary Reports” on page 318

For information about the Filter operators, see the following section:

- “Filter Operators” on page 319

Detailed Reports

The Detailed Report tab is the default view in the Report Layout region.



For a SSL-VPN Resource Activity report, the **Select report field** drop-down list contains four data categories that you can add as column headings in the report. The categories are:

- **Destination IP** – Adds a column containing the IP address of each accessed resource
- **Protocol** – Adds a column containing the protocol used by the traffic
- **Source IP** – Adds a column containing the IP address of each system which accessed a resource
- **User** – Adds a column containing the user ID

To include a field in the report, select a choice from the list and then click **Add**. When you click **Add**, a row is populated in the table below, which has three column headings: Field, Filter, and Options.

Note When you place your mouse cursor over the row, under the Field heading, the cursor changes to a “move” cursor. You can drag and drop the rows to rearrange the column ordering in the final report.

In the Filter column, two fields are displayed: an operator field and an input field. The operator field is a drop-down list containing the operator choices for the selected report field. See “Filter Operators” on page 319 for a description of each operator. The input field can be a drop-down list or a standard input field, depending on the selected report field.

The operators and input fields are defined in Table 7 for each report field.

Table 7 Operators and Input Fields for Each Data Type

Data Type	Operators	Input Field
Destination IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain destination IP address.
Protocol	Equals Start with End with Contains	The input field is a standard input field where you can type in the protocol to match, such as FTP. Leave the input field blank if you choose not to filter by a certain protocol.
Source IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain source IP address.
User	Equals Start with End with Contains	The input field is a standard input field where you can type in the user ID to match. Leave the input field blank if you choose not to filter by a certain user.

In the Options column, two icons are displayed: an Eye and an X . You can click the Eye to toggle whether the report field on that row will be displayed in the final report. This allows you to filter the report results based on the selected report field and related filter value, but not display the field as a column. When you click on the Eye icon within a row, the eye closes to show that this field will not be displayed in the final report. The filter value will still be used to filter results from the raw syslog database to apply towards the report.

For example, you might specify the following Field/Operator/Filter Value: **Protocol/=/http**. It would make sense to click the Eye icon to disable the Protocol field from being shown in the report, since it would always just be “http” and would not add any interesting information to the final report. Contrast this with simply specifying the Protocol field and leaving the Filter Value blank, in which case you would want to enable the Eye so that this column would appear in the report showing a variety of protocols such as udp/dns, tcp/http, udp/ntp, or numbered protocols such as udp/389 (the LDAP protocol) or tcp/445 (MS Server Message Block (SMB) file sharing).

Clicking the X icon under Options deletes the selected report field from the table, so it will not be used to generate the report results nor will it be displayed in the report. Use the X icon instead of the Eye when you do not choose to filter the report results based on the field.

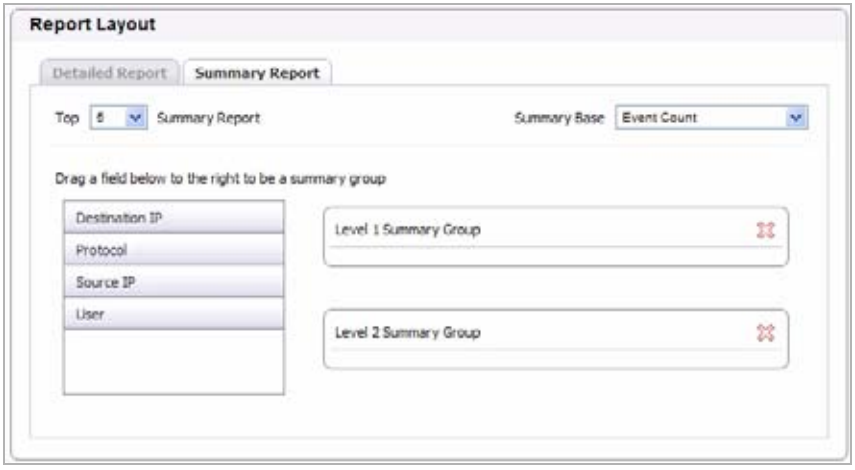
The Detailed Report tab also contains the Sort By drop-down list. The list contains the Date/Time option and any other report fields that you have selected from the eight data types. The choice you select will be used to order the results in the report from the first page to the last. The selection in the left drop-down list is used for the first sorting, then the selection in the right drop-down list is used to sort and group the entries within each group resulting from the the first sorting.

To configure a detailed report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Detailed Report** tab.
3. In the **Select report field** drop-down list, select a data type to include in the report, and then click **Add**. A row for this field is populated in the table below. Repeat this step to add other fields.
4. Optionally select an operator from the drop-down list under **Filter** in a table row, and type in or select an input value to be matched when the database is queried. Repeat this step for other rows to add filter values for those fields.
5. To prevent a field from appearing in the final report, click the **Eye** icon in that row so that the eye appears closed. To allow the field to be displayed in the report, click the closed **Eye** icon to return it to normal appearance.
6. To delete a field from the table, click the **X** icon in that row.
7. To sort the report pages by a different field than the default of Date/Time, select the desired field from the **Sort by** drop-down list.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region and the Report Layout region back to default settings.

Summary Reports

The Summary Report tab is available in the Report Layout region of the Template Section.



The Top drop-down list provides selections for the number of entries to display in the report. For example, if the User field is selected below as a Summary Group, and 5 is selected in the Top drop-down list, the report will provide entries for the top five users. For all Custom Reports, available numbers in the Top drop-down list are 5, 10, 20, 50, and 100.

The Summary Base drop-down list offers a selection of traffic types that will be used to determine the top usage for the selected field. For a SSL-VPN Resource Activity report, the only Summary Base choice is **Event Count**.

Below the Top and Summary Base fields, you can create one or two Summary Groups from the choices listed on the left side. For a SSL-VPN Resource Activity report, the choices are **Destination IP**, **Protocol**, **Source IP**, or **User**.

To select a field for a Summary Group, simply drag and drop the desired field from the list to either the Level 1 Summary Group or Level 2 Summary Group boxes. When the field name is dragged to one of these, the operator drop-down list and filter input value field are displayed, allowing you to specify values to match when the data is searched. See “Filter Operators” on page 319 for a description of each operator.

Either the Level 1 Summary Group field or the Level 2 Summary Group field can be used alone; the resulting report will look the same in both cases.

When both the Level 1 and Level 2 Summary Group fields are populated, the report will display the top entries for the Level 2 field for each of the top entries for the Level 1 field. For example, if User is dragged to the Level 1 Summary

Group and Domain is dragged to the Level 2 Summary Group, and 5 is selected in the Top drop-down list, the generated report will display the top five domains visited by each of the top five users.

To configure a summary report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Summary Report** tab.
3. In the **Top** drop-down list, select the number of entries to be displayed in the report.
4. In the **Summary Base** drop-down list, use the default, **Event Count**.
5. To specify the field for the **Level 1 Summary Group**, click and drag the desired field from the list on the left to the **Level 1 Summary Group** field, and then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.

6. To specify the field for the **Level 2 Summary Group**, click and drag the desired field from the list on the left to the **Level 2 Summary Group** field, then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.
7. To specify a filter operator and filter value for a Summary Group, select the operator from the drop-down list next to the field and type a filter value into the input field to the right of the operator.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region as well as the Report Layout region back to default settings.

Filter Operators

When configuring the Report Layout on either the Detailed Report tab or the Summary Report tab, you can specify filter values to be matched in the database during report generation. Depending on the selected field type, text string or numeric, several filter operators are available. The filter operators are used with a filter input value to determine which data should be included in the report.

The operators are defined as shown in Table 8.

Table 8 Filter Operators

Operator	Definition
Equals	Only data that exactly matches the filter input text will be included in the report
Start with	Data that begins with the input text will be included in the report
End with	Data that ends with the input text will be included in the report
Contains	Data that contains the input text will be included in the report
=	Only data that exactly matches the filter input numerical value will be included in the report
>	Data values that are greater than the input numerical value will be included in the report
>=	Data values that are greater than or equal to the input numerical value will be included in the report
<=	Data values that are less than or equal to the input numerical value will be included in the report
<	Data values that are less than the input numerical value will be included in the report
!=	Data values that are not equal to the input numerical value will be included in the report

Generating the Custom Report

The Generate Report button at the bottom of the Template Section is used to create the report. Before clicking Generate Report, use the Template Section to specify the time period for the report and the contents and layout of the report.

Note Custom Reports are available at the unit level and Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see “Viewing the SSL-VPN Log” on page 332.

To generate a custom report:

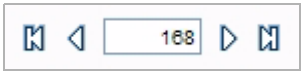
1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report you want.

2. In the **Date/Time** region of the Template Section, specify the time period that the report will cover. For detailed information and instructions, see “Configuring the Date and Time for Custom Reports” on page 311.
3. In the **Report Layout** region of the Template Section, specify the contents and appearance of the report. For detailed information and instructions, see “Configuring the Report Layout and Generating the Report” on page 314.
4. Click **Generate Report** to create the report using the specified configuration.

Viewing a Custom Report

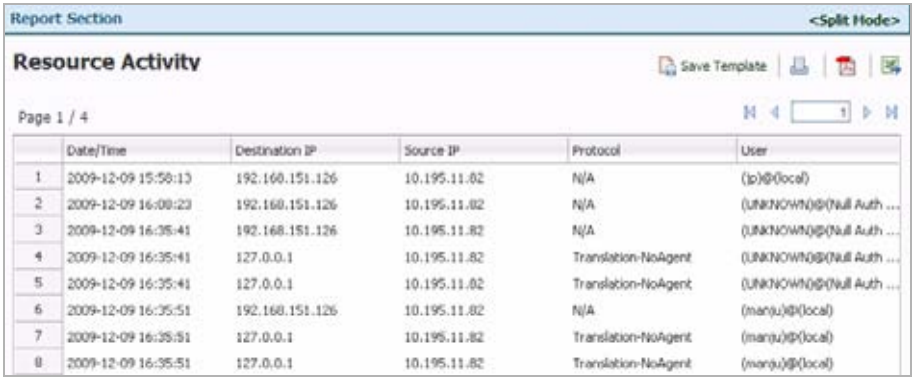
After you click Generate Report, the Report Section is displayed in Split Mode in the lower half of the main window, even if you previously were in Full Mode for the Template Section.

Pagination controls are displayed at the upper right of the report, just below the Save Template button and the printer, PDF, and Excel icons. Navigation buttons are provided to take you to the first page, next page, previous page, and last page, or you can specify an exact page number in the field.



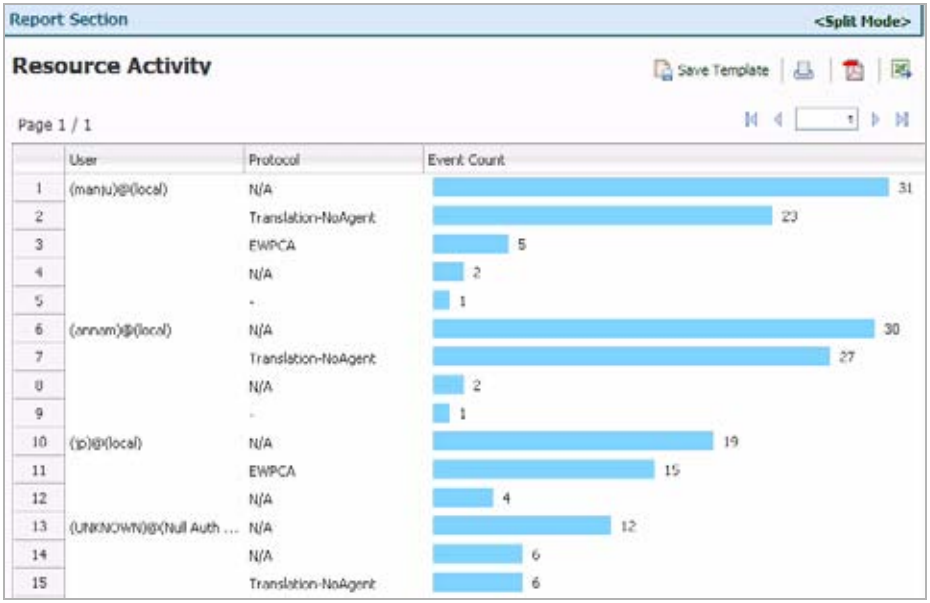
In a Detailed Report, the selected report fields are displayed as column headings. You can click on any column heading to sort that page by the values in the column that you click. Click again to toggle between ascending and descending order on that page. When you navigate away from that page and

then come back using the pagination controls, the page reverts to the original sorting order as specified in the **Sort by** field of the Template Section before generating the report.



	Date/Time	Destination IP	Source IP	Protocol	User
1	2009-12-09 15:58:13	192.168.151.126	10.195.11.82	N/A	(ip)@(local)
2	2009-12-09 16:09:23	192.168.151.126	10.195.11.82	N/A	(UNKNOWN)@(Null Auth ...
3	2009-12-09 16:35:41	192.168.151.126	10.195.11.82	N/A	(UNKNOWN)@(Null Auth ...
4	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	(UNKNOWN)@(Null Auth ...
5	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	(UNKNOWN)@(Null Auth ...
6	2009-12-09 16:35:51	192.168.151.126	10.195.11.82	N/A	(manju)@(local)
7	2009-12-09 16:35:51	127.0.0.1	10.195.11.82	Translation-NoAgent	(manju)@(local)
8	2009-12-09 16:35:51	127.0.0.1	10.195.11.82	Translation-NoAgent	(manju)@(local)

In a Summary Report, the Report Section displays the event count as horizontal bar charts. This lets you see the information at a glance, such as who had the most resource activity and which protocols they used the most.

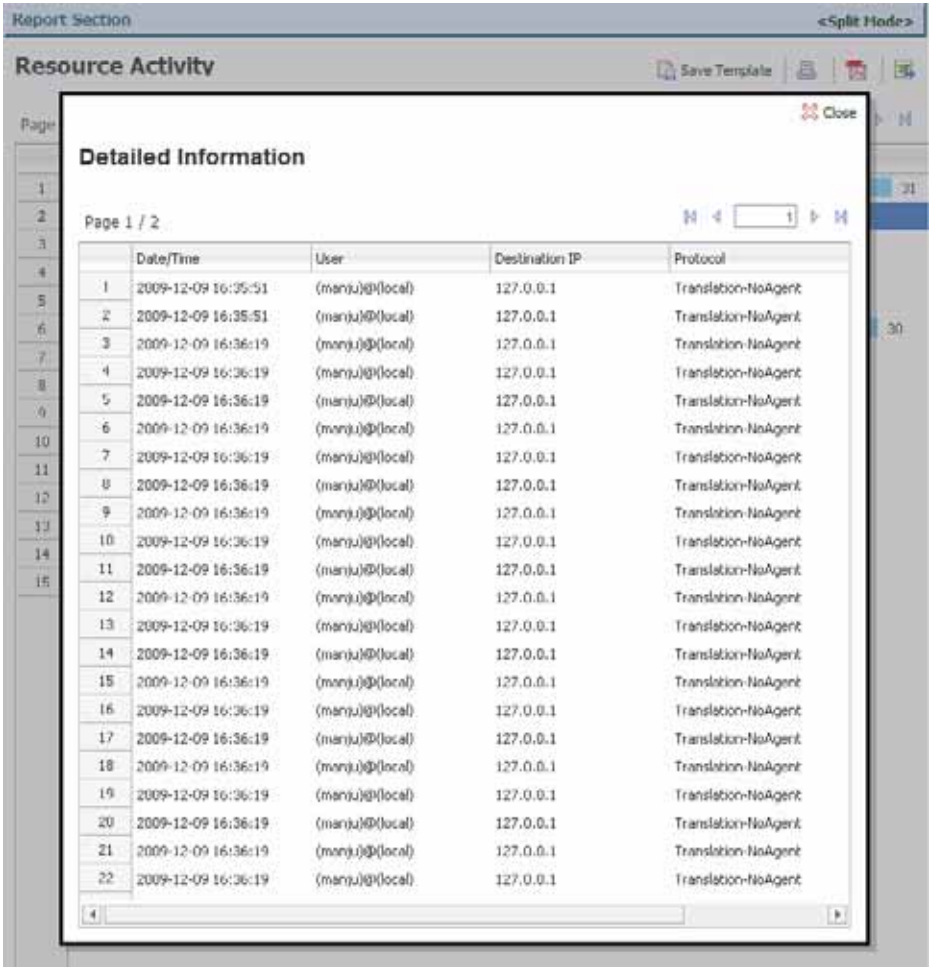


	User	Protocol	Event Count
1	(manju)@(local)	N/A	31
2		Translation-NoAgent	23
3		EWPCA	5
4		N/A	2
5		-	1
6	(anram)@(local)	N/A	30
7		Translation-NoAgent	27
8		N/A	2
9		-	1
10	(ip)@(local)	N/A	19
11		EWPCA	15
12		N/A	4
13	(UNKNOWN)@(Null Auth ...	N/A	12
14		N/A	6
15		Translation-NoAgent	6

You can click on a bar in the chart to pop up detailed information, just like the detailed report with all of the columns for all fields. The report lists details about this Summary Group field only. For example, if the Summary Group contains the User field and you click on a bar for one of the top users, the report displays the date and time of all resource activity for the user, and

includes data for every field available for detailed reports. A scroll bar is provided along the bottom of the Detailed Information window to allow viewing of all four fields plus the date and time column.

The Detailed Information window is shown below.



Printing a Page or Exporting the Report as a PDF or CSV File

To print the current page of the report, click the printer icon at the top of the Report Section. Your normal print dialog box pops up. This prints only the page that is currently displayed.

To export the entire report in PDF format, click the PDF icon at the top of the Report Section. A PDF file is generated showing the report results in table format.

To export the entire report in Microsoft Excel Comma Separated Value (CSV) format, click the Excel icon at the top of the Report Section. A CSV file is generated showing the report results in spreadsheet format.

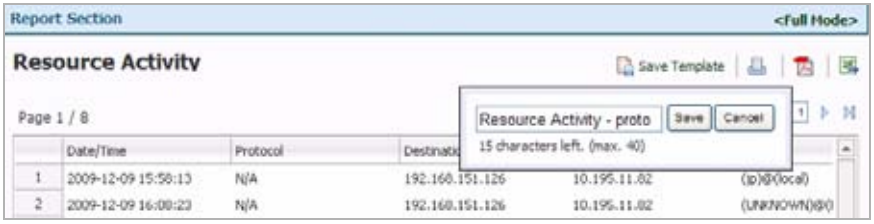
The PDF can contain a maximum of 10,000 records. If your report contains more than 10,000 records, you can use the Static Date Range fields to adjust the dates and regenerate the report to shorten its length. You can save the PDF or CSV file using any filename and location.

Saving the Report Template

After generating the report, you can save the settings for this report as a template for reuse. You can select the saved template from the Template Section at a later time, and use it to generate a report using the same settings. The template is saved for the currently selected appliance and for the specific user. The saved template will not be available for other appliances or for other users.

To save the report template:

1. In the Report Section in the upper right corner, click the **Save Template** button.



2. In the popup dialog box, type in a descriptive name for the template, up to 40 characters. The number of remaining characters allowed in the name is displayed below the input field and changes as you type.
3. Click **Save**. If you are in a Full Mode display of the Report Section, you can verify that the template has been saved by changing back to Split Mode and viewing the contents of the **Template** drop-down list.

Viewing SSL-VPN Resources Reports

Resources reports provide information on the amount of data transmitted through the selected SSL-VPN appliance by each service or protocol.

Resources reports are useful for revealing inappropriate usage of bandwidth and can help determine network policies. For example, if there is a large spike of bandwidth usage, you can determine whether this is caused by regular Web access, someone using FTP to transfer large files, an attempted Denial of Service (DoS) attack, or another service.

Note All reports appear in the appliance's time zone.

The procedures for viewing the Resources Reports are described in the following sections:

- "Viewing SSL-VPN Resources Summary Reports" on page 325
- "Viewing SSL-VPN Resources Top Users Reports" on page 327

Note You cannot view resources reports from the global view.

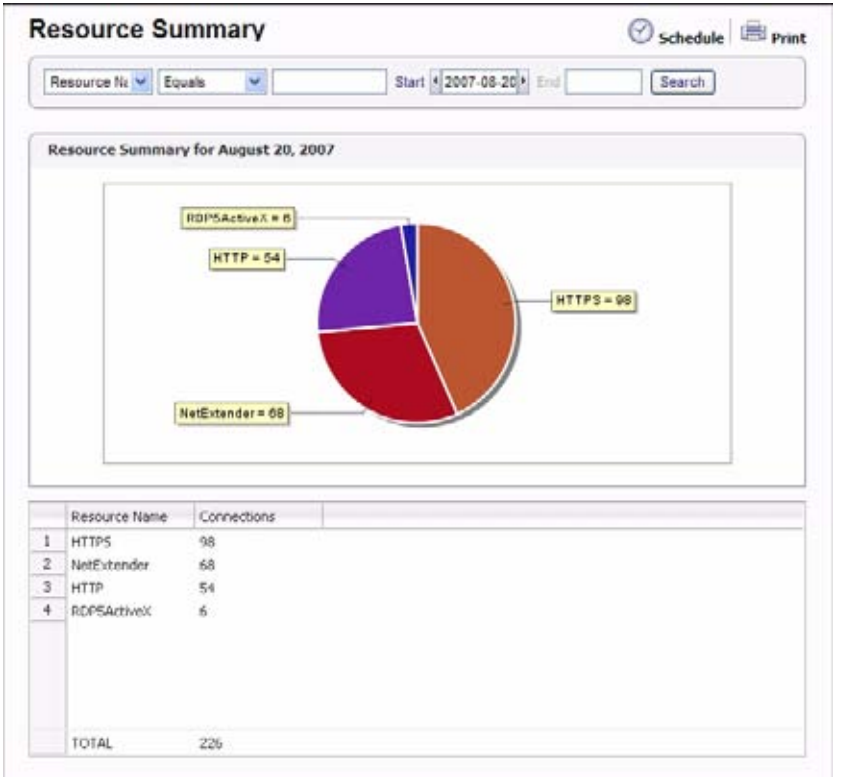
Viewing SSL-VPN Resources Summary Reports

The Resources Summary report displays the number of connections handled by each service or protocol during the specified day.

To view the Resources Summary report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.

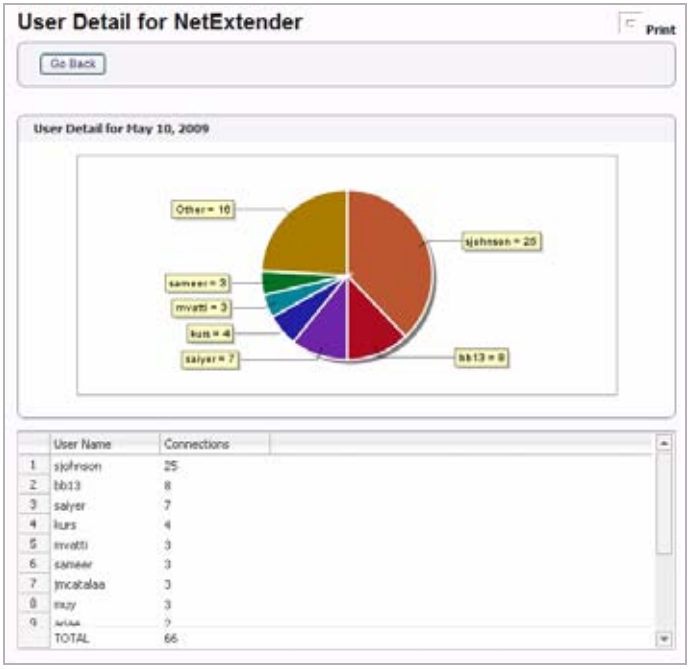
3. Expand the **Resources** tree and click **Summary**. The Resources Summary page displays.



4. The graph displays the number of connections used by each service or protocol during the day.
5. The table contains the following information:

- **Resource name**—the service or protocol
- **Connections**—number of connection events or “hits”

6. To view the user detail for a particular resource, click the resource slice in the pie chart or the resource name in the table to drill down for this information.



7. To return to the Resources > Summary page, click the **Go Back** button.
8. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
9. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date.

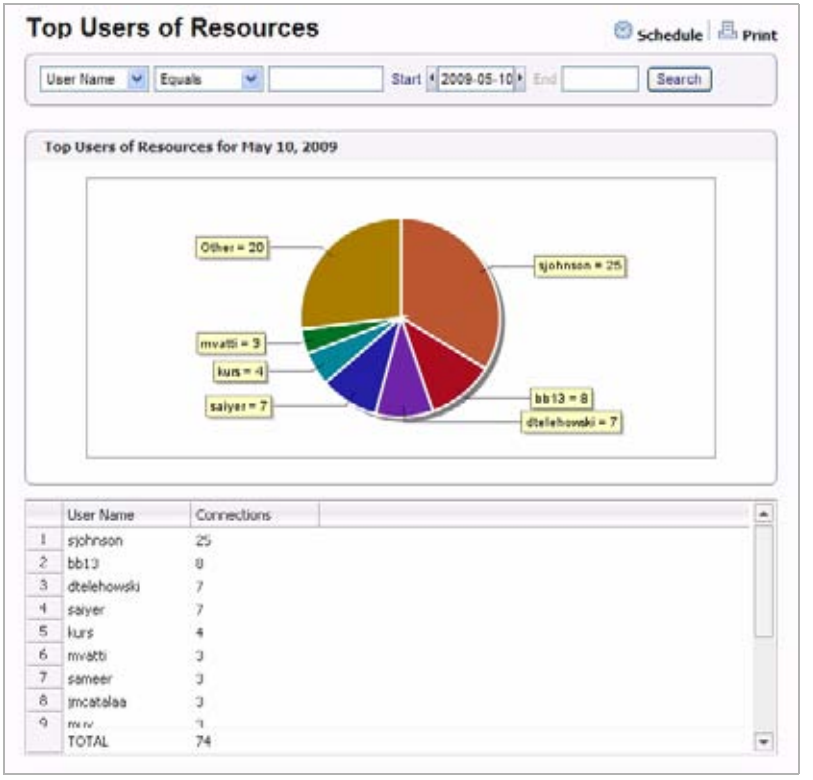
Note This date setting will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Resources Top Users Reports

The Resources Top Users report displays the users who used the most connections on the specified date.

To view the Resources Top Users report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Resources** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of connections used by each user.
5. The table contains the following information for all users:
   - **Users**—the user name
   - **Connections**—number of connection events or “hits”

6. To view the resources by service or protocol used by a particular user, click the user slice in the pie chart or the user name in the table to drill down for this information.

7. To return to the Resources > Top Users page, click the **Go Back** button.
8. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart for the top six users, and a table for all users. To change the date of the report, click the **Start** field to access the drop-down calendar.
9. To display a limited number of users, use the Search Bar fields.

Note The search bar fields use pattern matching with operators such as "contains". For example, "john" will match john_smith, john42, or big_john.

10. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note The date setting will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Authentication Reports

The Authentication reports show user logins and failed login attempts. Authentication reports are available at the unit level.

Note All reports appear in the appliance's time zone.

Select from the following:

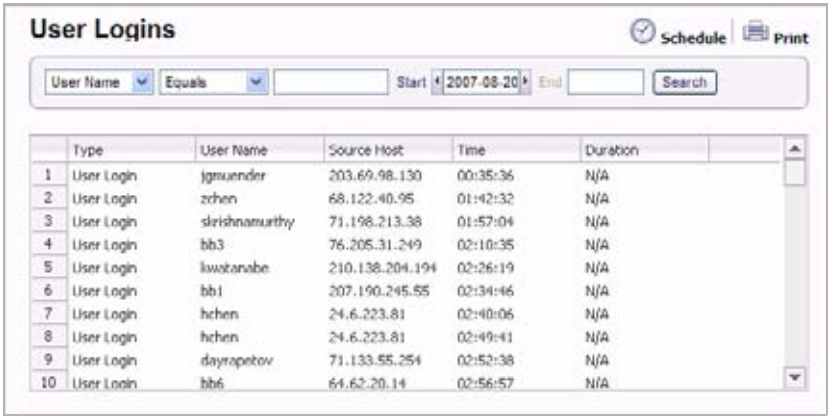
- "Viewing SSL-VPN User Login Reports" on page 330
- "Viewing SSL-VPN Failed Login Reports" on page 331

Viewing SSL-VPN User Login Reports

The user login report shows the user name, source host IP address, and time of login for users that logged on to the SSL-VPN appliance during the specified day.

To view the User Login report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Authentication** tree and click **User Login**. The User Login page displays.



4. The table contains the following information:
   - **Type**—equal to User Login
   - **User Name**—the user name

- **Source Host**—the IP address of the user's computer
- **Time**—the time that the user logged in
- **Duration**—the duration of the user login session

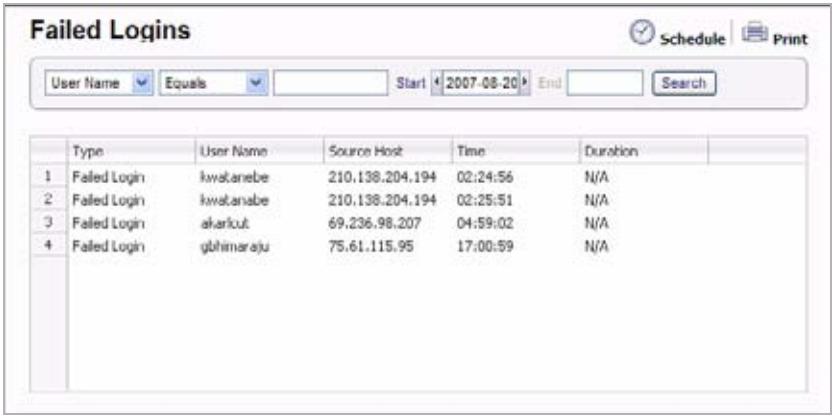
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing SSL-VPN Failed Login Reports

The failed login report shows failed login attempts for users who attempted to log into the SSL-VPN appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Authentication** tree and click **Failed Login**. The Failed Logins page displays.



4. The table contains the following information:
   - **Type**—equal to Failed Login
   - **User Name**—the user name
   - **Source Host**—the IP address of the user's computer
   - **Time**—the time that the user attempted to log in

- **Duration**—not applicable

5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the SSL-VPN Log

The Log Viewer contains detailed information on each transaction that occurred on the SSL-VPN appliance. This information is stored for the time that you specified in the configuration settings.

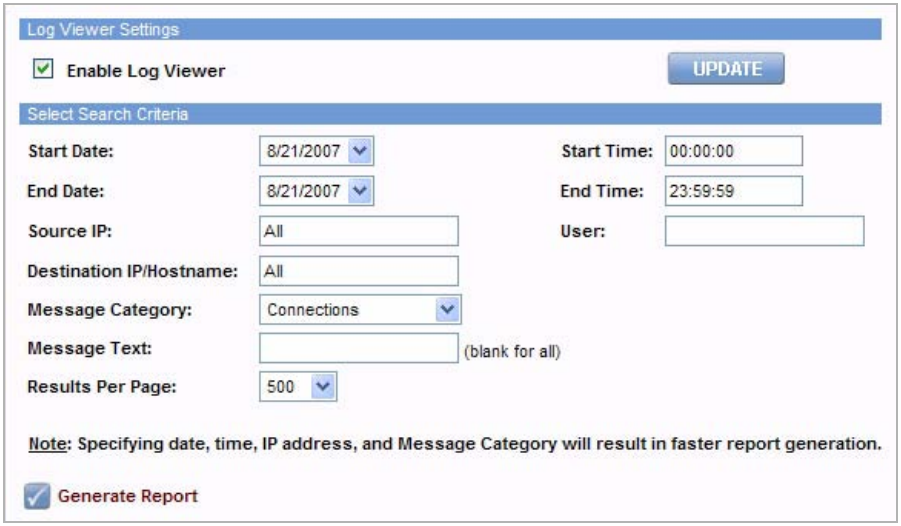
Note The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For more information, see "Scheduling and Configuring Reports" on page 133.

Viewing the Log for a SSL-VPN Appliance

To view the Log, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.

3. Expand the **Log Viewer** tree and click **Search**. The Search page displays.



4. Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer.
5. Under Select Search Criteria, select the date range to view data from in the **Start Date** and **End Date** fields.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.
8. To limit the report to data originating from specific IP addresses, enter the source IP address in the **Source IP** field. To view all IP addresses, enter **All**.
9. To view log entries for data originating from a particular user, enter the user name in the **User** field.
10. To limit the report to data going to specific IP addresses or hosts, enter the destination IP address or host name in the **Destination IP/Hostname** field. To view data for all IP addresses, enter **All**.
11. Select the type of events to view from the **Message Category** list box. You can select from the following:
    - All Categories
    - Connections
    - Rejected Connections

- User Events
- Unrecognized Events

12. To limit the report to messages containing a specific text string, enter the text in the **Message Text** field. Leave the field blank to view all messages.
13. Select the number of entries to display per page from the **Results Per Page** field.
14. Click **Generate Report**. The Log Search Results page displays.

Log Search Results for August 23, 2007 00:00:00 to August 23, 2007 23:59:59 as of 08/23/2007 19:45:11 UTC
Message Category: Connections
Displaying records 1-500 of 1015 Next 500
Time
Source
Destination
User
Resource
Message
08/23/2007 23:58:17 71.142.77.166 204.110.31.44 jalvarez NetExtender NetExtender
08/23/2007 23:57:32 71.142.77.166 204.110.31.44 jalvarez NetExtender NetExtender
08/23/2007 23:56:24 71.142.77.166 10.50.14.117 jalvarez RDPSActiveX Terminal Services
08/23/2007 23:56:05 71.142.77.166 204.110.31.44 jalvarez NetExtender NetExtender
08/23/2007 23:55:23 71.142.77.166 204.110.31.44 jalvarez NetExtender NetExtender
08/23/2007 23:54:06 71.142.77.166 204.110.31.44 jalvarez NetExtender NetExtender
08/23/2007 23:53:33 75.24.111.94 10.50.128.206 cye HTTPS HTTPS Connection
08/23/2007 23:53:33 75.24.111.94 10.50.128.206 cye HTTPS HTTPS Connection
08/23/2007 23:53:33 75.24.111.94 10.50.128.206 cye HTTPS HTTPS Connection
08/23/2007 23:53:33 75.24.111.94 10.50.128.206 cye HTTPS HTTPS Connection

15. To view the next page of entries, click **Next**.
16. To generate another report, click **Search** again in the **Log Viewer** tree.

Appendix A

Installing SonicWALL ViewPoint

This appendix is designed to help you install SonicWALL ViewPoint. If you have not used SonicWALL ViewPoint before, you might want to familiarize yourself with SonicWALL ViewPoint concepts and features. This appendix contains the following sections:

- "About Installing and Upgrading SonicWALL ViewPoint" section on page 336
- "Activating SonicWALL ViewPoint on Your Appliances" section on page 340
- "Installing Universal Management Suite" section on page 342
- "Upgrading SonicWALL ViewPoint 5.1 to 6.0" section on page 349
- "Registering SonicWALL ViewPoint" section on page 351
- "Configuring Deployment Settings" section on page 354
- "Upgrading from ViewPoint to GMS" section on page 356
- "Miscellaneous Procedures and Troubleshooting Tips" section on page 368

About Installing and Upgrading SonicWALL ViewPoint

You can either perform a fresh installation of SonicWALL ViewPoint using the installer or upgrade a previous installation of SonicWALL ViewPoint, patched or unpatched.

The upgrade installer checks with the SonicWALL backend to see if the SonicWALL ViewPoint deployment has valid support. If it does not, then the upgrade discontinues. When the SonicWALL ViewPoint installer detects that the SonicWALL backend site is not accessible, it prompts the user to enter an Upgrade Key.

If the key is valid, it allows the upgrade to continue. If the key is invalid, the installation fails.

Note The upgrade key can be obtained by contacting SonicWALL Technical Support.

Installing SonicWALL ViewPoint

This chapter describes how to install or upgrade SonicWALL ViewPoint.

To install or upgrade SonicWALL ViewPoint, complete the following procedures:

- Review the installation requirements. See “Installation Overview” on page 336.
- To install SonicWALL ViewPoint, see “Installing Universal Management Suite” on page 342.

Installation Overview

The SonicWALL ViewPoint Installation program is an HTML-launched installer that automatically detects whether you are installing on Windows Server 2000/2003/2008. After the installation program detects the operating system, the installation procedure is identical.

System Requirements

Note SonicWALL does not support installations of ViewPoint running on any virtualization software, such as VMware.

Before installing SonicWALL ViewPoint, review the requirements in the following sections:

- Operating System Requirements, page 337
- Database Requirements, page 337
- Java Requirements, page 338
- Browser Requirements, page 338
- Hardware Requirements, page 339
- SonicWALL Appliance and Firmware Support, page 339
- Network Requirements, page 339
- MySonicWALL Account Requirements, page 340

Operating System Requirements

In order to install and run SonicWALL ViewPoint, you must be logged in as the administrator. SonicWALL ViewPoint is supported on the following operating systems:

- Windows Server 2008 SBS, 64-bit
- Windows Server 2008 Standard (SP1), 32-bit and 64-bit
- Windows Server 2003 (SP2), 32-bit and 64-bit
- Windows Server 2000 (SP4)
- Windows 7, 32-bit and 64-bit
- Windows Vista (SP1), 32-bit and 64-bit
- Windows XP Professional (SP3), 32-bit

In all instances, SonicWALL ViewPoint runs as a 32-bit application.

Database Requirements

For fresh installations or after upgrading from 5.1, SonicWALL ViewPoint 6.0 supports the following database:

- MySQL 32-bit version 5.0.83 for Windows, bundled with SonicWALL ViewPoint 5.1 and above

The MySQL 5.0 separate installer that was provided with SonicWALL ViewPoint 5.0 is still supported.

The requirements for the MySQL server are as follows:

- Windows 2000 (SP4) and newer Windows operating systems
- Minimum 300 GB hard disk space
- Minimum 2 GB RAM
- NTFS file system
- Not a Virtual Machine (VM)

After upgrading from 5.1, SonicWALL ViewPoint 6.0 supports the following databases only when the database was already in use prior to upgrading:

- Microsoft SQL Server 2005 (SP2), 32-bit and 64-bit, as follows:
  - SQL Server 2005 Workgroup
  - SQL Server 2005 Standard
  - SQL Server 2005 Enterprise
  - SonicWALL ViewPoint does not support Microsoft SQL 2005 Express
- Microsoft SQL Server 2000 (SP4)
- Microsoft Desktop Engine (MSDE) bundled with ViewPoint

Java Requirements

Java Plug-in version 1.6 or higher is required on client machines when accessing the SonicWALL ViewPoint application interface. SonicWALL Universal Management Suite (UMS) automatically downloads the latest Java Plug-in. SonicWALL UMS services use JRE 1.6. For the Web server, SonicWALL UMS uses Tomcat 6.0.20.

Browser Requirements

- Microsoft Internet Explorer 6.0 or higher
- Mozilla Firefox 2.0 or higher
- Pop-up blocker disabled

SonicWALL ViewPoint supports SSL 3.0 / TLS 1.0 for HTTPS direct login to SonicWALL appliances from SonicWALL ViewPoint. For enhanced security across a SonicWALL ViewPoint network for installations that must comply with stringent regulatory compliance and account management controls as found in such standards as PCI, SOX, or HIPAA, the following browsers have SSL 3.0/TLS 1.0 as standard encryption protocols:

- Microsoft Internet Explorer 7.0 or higher

- Mozilla Firefox 2.0 or higher

Hardware Requirements

The hardware platform where SonicWALL ViewPoint is installed must meet the following requirements:

- x86 environment
- 3 GHz or faster single-CPU Intel processor
- Minimum 2 GB RAM
- At least 100 GB of free disk space

Note Ensure that the drive where SonicWALL ViewPoint is installed has ample space to store the SonicWALL ViewPoint log files.

SonicWALL ViewPoint requires large amounts of disk space for database storage. In early versions, the maximum raw syslog database size was 2 GB. SonicWALL ViewPoint now provides enhanced database capacity by creating a new 2 GB database everyday. Each file name includes the date it was created for easy reference.

SonicWALL Appliance and Firmware Support

You can use SonicWALL ViewPoint reporting for the following SonicWALL security appliances:

- SonicWALL firewalls running SonicOS 1.0 or higher, or SonicWALL firmware 6.1.2.0 or higher
- SonicWALL SSL-VPN 200 / 2000 / 4000 running SonicOS SSL VPN 2.1 or higher
- SonicWALL SRA 4200 running SonicOS SSL VPN 3.5.0.11 or higher
- SonicWALL Aventail E-Class SRA EX-Series appliances running version 9.0 or higher
- SonicWALL CSM Series running SonicOS CF 1.0 or higher

Network Requirements

To complete the SonicWALL ViewPoint deployment process, the following network requirements must be met:

Syslog and SNMP Port Settings

You should either disable your personal firewall, or enable ports for syslog, syslog forwarding, and SNMP traps. The default syslog port is UDP 514 and the default SNMP port is UDP 162.

If the SonicWALL ViewPoint system is behind a gateway or firewall, you may need to open up these ports on that device.

Static IP / DHCP

If accessed from the WAN interface, the SonicWALL appliance must have a static IP address. Otherwise, it may have either a static or dynamic IP address.

HTTP / HTTPS

HTTP and HTTPS access for adding a SonicWALL appliance to ViewPoint is supported as follows:

- HTTP for access to a LAN IP address only
- HTTPS for access to a LAN IP or WAN IP address

MySonicWALL Account Requirements

A MySonicWALL account is required to complete the SonicWALL UMS installation and registration process. If you do not already have a MySonicWALL account, open a Web browser and navigate to the following website:

http://www.mysonicwall.com

Follow the on-screen prompts to create a user account.

Activating SonicWALL ViewPoint on Your Appliances

To use SonicWALL ViewPoint, you must license it on each SonicWALL security appliance for which you want reports. The SonicWALL appliance must be registered on MySonicWALL before you can purchase and activate the SonicWALL ViewPoint license for it. You must also enable the SonicWALL ViewPoint license on the appliance itself.

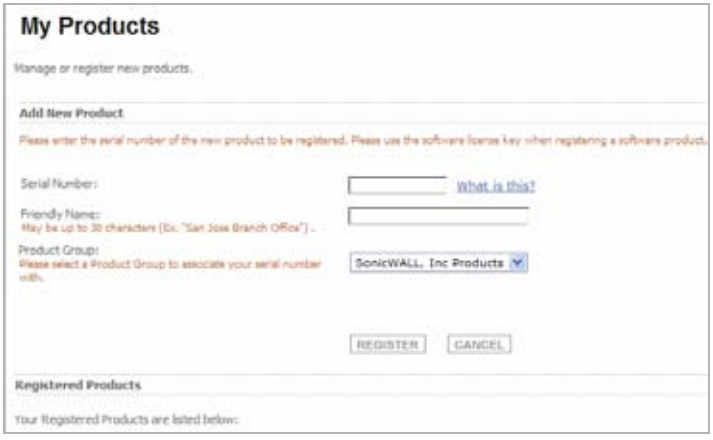
See the following sections:

- "Registering Your SonicWALL Appliance" on page 341
- "Activating the ViewPoint Software on Your Appliance" on page 341
- "Enabling the ViewPoint License on Your Appliance" on page 342

Registering Your SonicWALL Appliance

To register the SonicWALL appliance that ViewPoint will monitor, perform the following steps:

1. Log on to MySonicWALL.
2. Click **My Products**. The **SonicWALL My Products** page displays.


My Products
Manage or register new products.
Add New Product
Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product.
Serial Number:
What is this?
Friendly Name:
May be up to 30 characters (Ex. "San Jose Branch Office").
Product Group:
Please select a Product Group to associate your serial number with.
SonicWALL, Inc Products
REGISTER
CANCEL
Registered Products
Your Registered Products are listed below:

3. Enter your SonicWALL serial number in the **Serial Number** field.
4. Enter a descriptive name for the SonicWALL appliance in the **Friendly Name** field.
5. Select the **Product Group** from the drop-down list.
6. Click **Register**. The MySonicWALL website registers the SonicWALL appliance.

Activating the ViewPoint Software on Your Appliance

To activate the SonicWALL ViewPoint software, perform the following steps:

1. Log on to mysonicwall.com.
2. Click the label of the newly registered SonicWALL appliance. The Service Management page displays.
3. Scroll down to locate the ViewPoint service and click **Enter Key**. The Activate Service page displays.
4. Enter the ViewPoint Activation Key in the **Activation Key** field. The ViewPoint Activation Key is printed on the ViewPoint Software License Certificate shipped with the ViewPoint package. If you purchased ViewPoint on mysonicwall.com, the key is emailed to you.

5. Click **Submit**. After the Activation Key is registered, a ViewPoint License Key will appear. Carefully write down the ViewPoint License Key in a safe place.

Enabling the ViewPoint License on Your Appliance

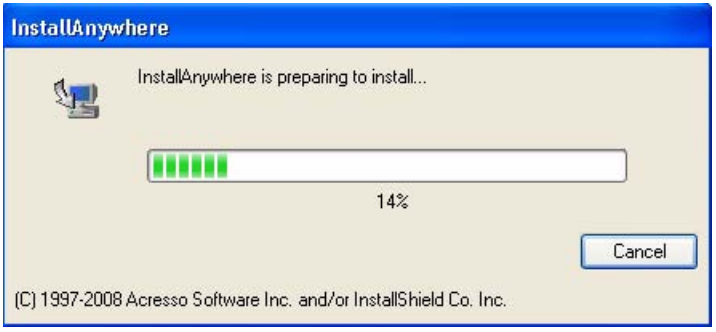
To enable the SonicWALL ViewPoint license, perform the following steps:

1. Log into the SonicWALL appliance.
2. Navigate to **Log > ViewPoint**. The **ViewPoint** page displays.
3. Enter the ViewPoint License Key provided by mysonicwall.com in the **Enter Upgrade Key** field.
4. Click **Apply**.
5. Restart the SonicWALL for the change to take effect.

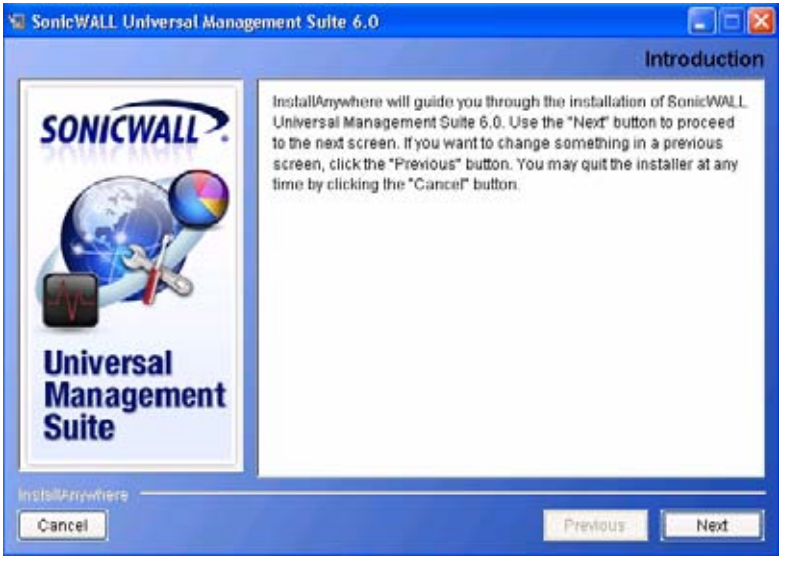
Installing Universal Management Suite

This section provides the procedures to install the SonicWALL Universal Management Suite (UMS) software. To install the SonicWALL UMS software, perform the following steps:

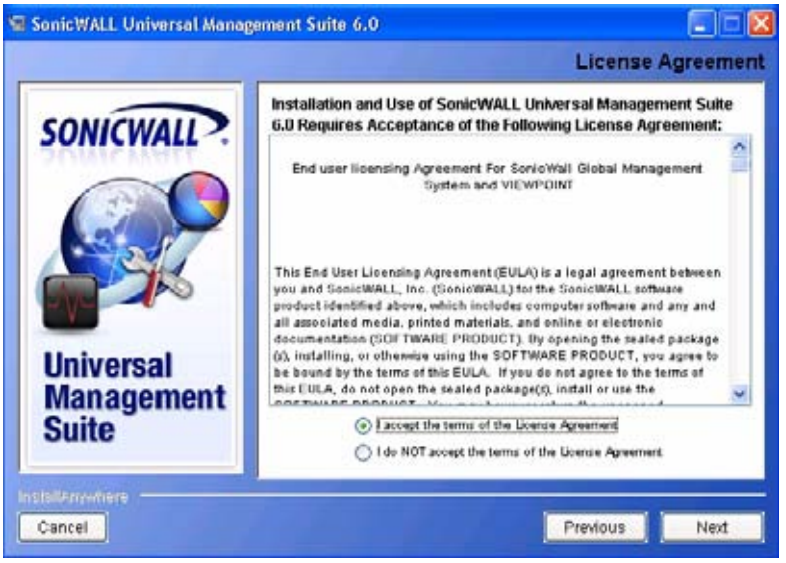
1. Log on to your SonicWALL ViewPoint management computer as **administrator** (Windows).
2. Run the SonicWALL ViewPoint installation file, **sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe** (where "xxxx" represent the exact version numbers). It may take several seconds for the InstallAnywhere installer to initialize.



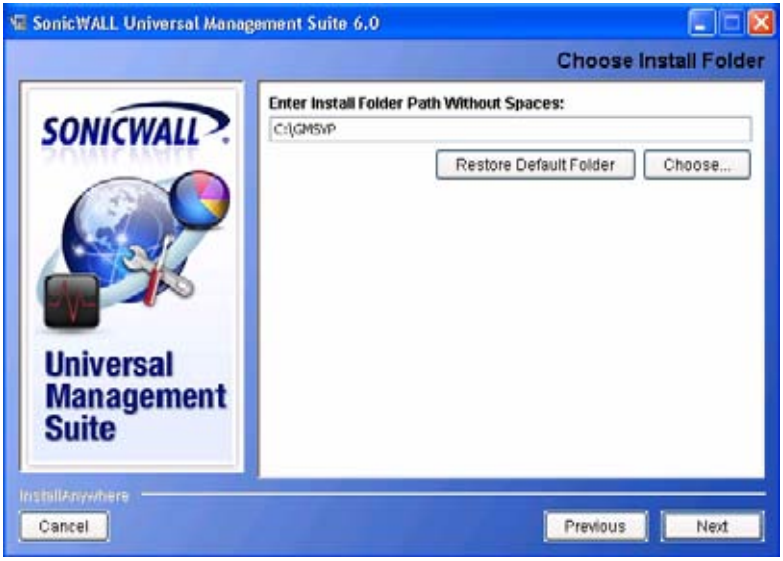
3. In the Introduction screen, click **Next**.


SonicWALL Universal Management Suite 6.0
Introduction
InstallAnywhere will guide you through the installation of SonicWALL Universal Management Suite 6.0. Use the "Next" button to proceed to the next screen. If you want to change something in a previous screen, click the "Previous" button. You may quit the installer at any time by clicking the "Cancel" button.
SONICWALL
Universal Management Suite
InstallAnywhere
Cancel
Previous
Next

4. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.

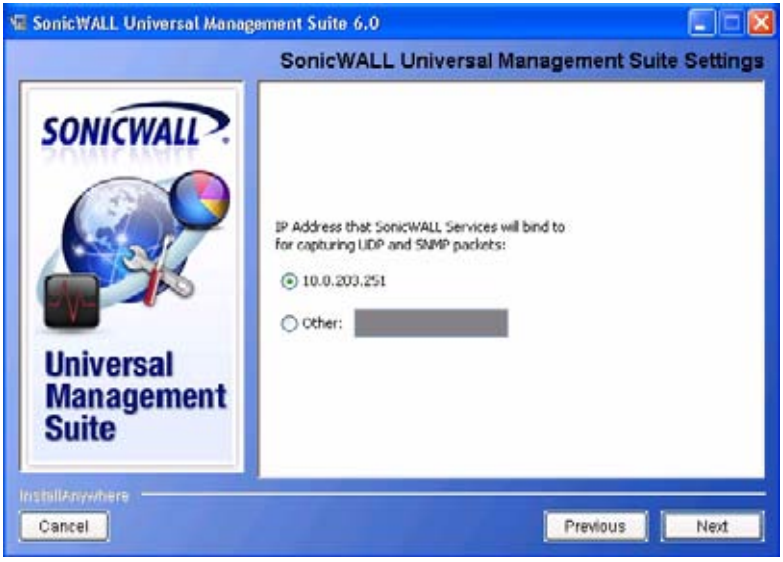

SonicWALL Universal Management Suite 6.0
License Agreement
Installation and Use of SonicWALL Universal Management Suite 6.0 Requires Acceptance of the Following License Agreement:
End user licensing Agreement For SonicWall Global Management System and VIEWPOINT
This End User Licensing Agreement (EULA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package (s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not open the sealed package(s), install or use the
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
SONICWALL
Universal Management Suite
InstallAnywhere
Cancel
Previous
Next

5. Select the path to the folder where you would like to install SonicWALL ViewPoint. You can accept the default path, **C:\GMSVP**, type in a new path, or click the **Choose** button to navigate to the selected folder. When you are finished, click **Next**.

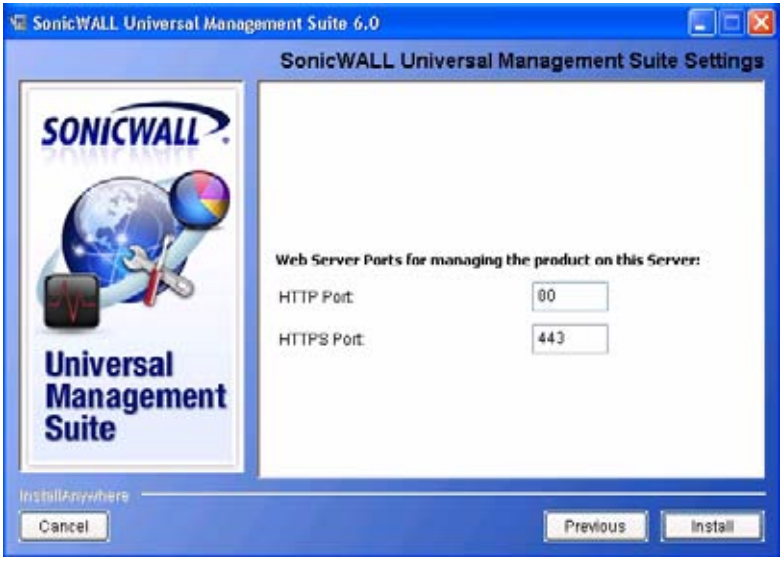


Tip Do not include spaces in the SonicWALL ViewPoint installation path.

6. Select the IP address you want SonicWALL Services to bind to for capturing syslog and SNMP packets. The default is your management computer IP address. To provide a different IP address, select the radio button next to **Other** and enter the IP address. Click **Next**.



7. In the SonicWALL Universal Management Suite Settings window, enter the Web server ports for HTTP and HTTPS.



Tip If you receive the message "Cannot bind to the port number specified. Please specify a different one," the port you specified in **Web Server Port** is in use by another program, for example, Internet Information Services (IIS). Specify another unused Web server port, for example, 8080.

Tip If you specify a custom port, you will need to modify the URLs you use to access SonicWALL ViewPoint by using the following format: **http://localhost:<port>/sgms/login** (to login from the local host) or **http://<***host_ipaddress***>:<port>/sgms/login** (to login from a remote location). For example, if you specified port 8080, the URL would be **http://localhost:8080/sgms/login** for a local host login, or **http://10.0.93.20:8080/sgms/login** for a remote login.

8. Click **Install**. You may see a Windows Firewall security alert. If you do, click **Unblock**.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: Java(TM) 2 Platform Standard Edition binary
Publisher: Sun Microsystems, Inc.
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

9. The Installer displays the installation progress during the few minutes required. Upon completion, whether or not the system has Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall. Click **OK**.

Syslogs/SNMP Capture
Syslogs/SNMP Capture
If you have a Personal Firewall software running on this system, please disable it for proper functioning of this product. Alternatively, you should enable ports for Syslogs (typically 514), Syslog Forwarding (typically 21007) and SNMP traps (typically 162) on the Personal Firewall.
Also, if you plan to enable any remote appliance for HTTPS Management, you will need to configure the Firewall/Gateway in front of this system to forward UDP Syslog (port 514) and SNMP (port 162) packets to this system.
Otherwise, this Universal Management system will not receive any Syslogs and SNMP traps for its proper functioning.
OK

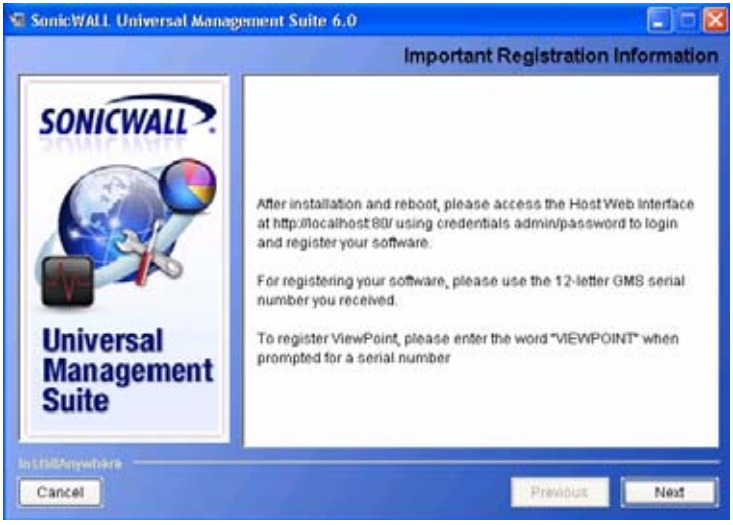
10. The Important Registration Information screen provides the URL and credentials to use to access the SonicWALL ViewPoint Universal Management Host system interface after restarting your system, as well as information about registration.

    The default URL for accessing the interface from the local system is:
    http://localhost:80/

    The default credentials are:
    User name – **admin**
    Password – **password**

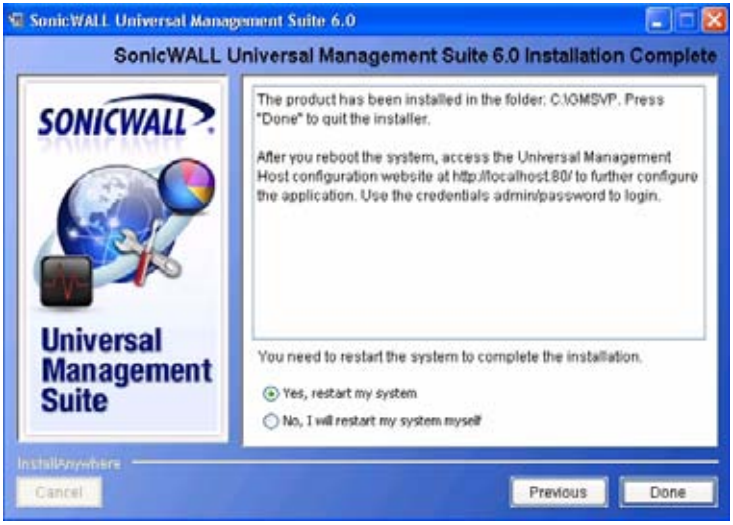
    To register for a SonicWALL ViewPoint installation, enter the word **VIEWPOINT** instead of a serial number when you register the product on MySonicWALL.

Click **Next**.


SonicWALL Universal Management Suite 6.0
Important Registration Information
SONICWALL
Universal Management Suite
After installation and reboot, please access the Host Web Interface at http://localhost:80/ using credentials admin/password to login and register your software.
For registering your software, please use the 12-letter GMS serial number you received.
To register ViewPoint, please enter the word "VIEWPOINT" when prompted for a serial number
InstallAnywhere
Cancel
Previous
Next

11. In the Installation Complete screen, select one of the following options for restarting your system to complete the installation, and then click **Done**:
    - **Yes, restart my system**
    - **No, I will restart my system myself**

Note Restarting after installation is required for full functionality.


SonicWALL Universal Management Suite 6.0
SonicWALL Universal Management Suite 6.0 Installation Complete
SONICWALL
Universal Management Suite
The product has been installed in the folder: C:\OMSVP. Press "Done" to quit the installer.
After you reboot the system, access the Universal Management Host configuration website at http://localhost:80/ to further configure the application. Use the credentials admin/password to login.
You need to restart the system to complete the installation.
Yes, restart my system
No, I will restart my system myself
InstallAnywhere
Cancel
Previous
Done

12. After restarting your system, you can access the SonicWALL ViewPoint UMH system interface by either clicking on the new desktop shortcut for **SonicWALL Universal Management Suite 6.0** or by pointing your browser at **http://localhost:80/**.
13. Your default Web browser will launch **http://localhost:80/appliance/login**.
14. Login using the username **admin** and the password **password**.
15. You will be prompted to change your password.

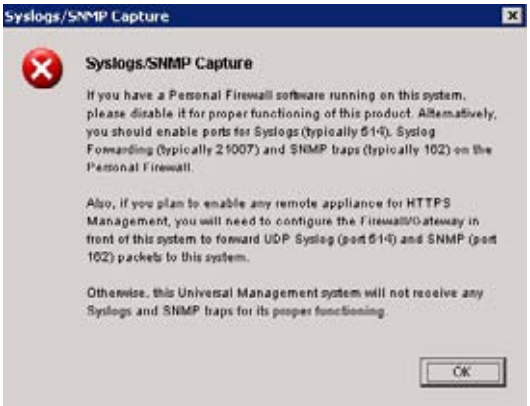
Note You are forced to change your password the first time you login.

Upgrading SonicWALL ViewPoint 5.1 to 6.0

To upgrade from SonicWALL ViewPoint 5.1 to 6.0 using the the Universal Management Suite 6.0 single binary installer, perform the following steps:

1. Log on to your SonicWALL ViewPoint management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 6.0 installer, by double-clicking the file **sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe** (where "xxxx" represent the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.
2. In the Introduction screen, click **Next**.
3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.
4. When the installer detects that SonicWALL ViewPoint 5.1 is currently installed on the system, a notification is displayed. Click **Install** to continue the upgrade.
5. The installer begins installing the files, using the existing installation folder, IP address to which SonicWALL Services bind for capturing syslog and SNMP packets, and Web port settings.

6. The Installer displays the installation progress during the few minutes required. Upon completion, whether or not the system has Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall. Click **OK**.


Syslogs/SNMP Capture
Syslogs/SNMP Capture
If you have a Personal Firewall software running on this system, please disable it for proper functioning of this product. Alternatively, you should enable ports for Syslogs (typically 514), Syslog Forwarding (typically 21007) and SNMP traps (typically 162) on the Personal Firewall.
Also, if you plan to enable any remote appliance for HTTPS Management, you will need to configure the Firewall/Gateway in front of this system to forward UDP Syslog (port 514) and SNMP (port 162) packets to this system.
Otherwise, this Universal Management system will not receive any Syslogs and SNMP traps for its proper functioning.
OK

7. The Important Registration Information screen provides the URL for access to the SonicWALL ViewPoint Universal Management Host system interface after upgrade completion, as well as information about registration.

   The default URL for accessing the interface from the local system is:
   http://localhost:80/

   The default credentials are:
   User name – **admin**
   Password – **password**

   To register for a SonicWALL ViewPoint installation, enter the word **VIEWPOINT** instead of a serial number when you register the product on MySonicWALL.

   Click **Next**.

8. The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click **Done**.

   In the SonicWALL ViewPoint login page, enter the same credentials for **User** and **Password** that you had in your earlier version prior to the upgrade.

Registering SonicWALL ViewPoint

SonicWALL ViewPoint registration is performed using the Universal Management Host system management interface. The first time you log into the system interface, the System > Status page will display a **Registration Pending** notification at the top of the screen, and the **Register** button will be available in the top right corner of the interface.

SonicWALL ViewPoint must be registered before you can use it. To complete registration, SonicWALL ViewPoint must have access to the Internet. The SonicWALL ViewPoint registration process sends your registration information to the MySonicWALL registration site. When registration is completed, SonicWALL ViewPoint will be licensed on your system.

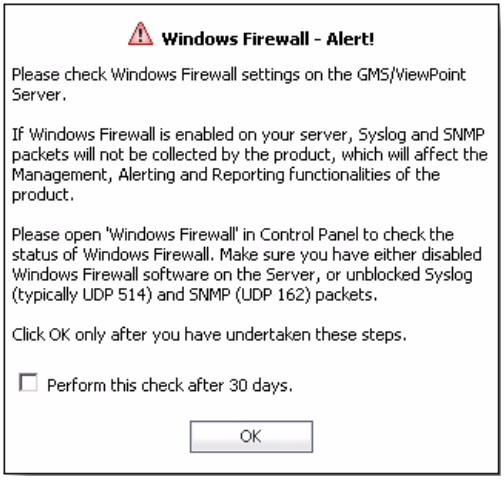
Note MySonicWALL registration information is not sold or shared with any other company.

To register SonicWALL ViewPoint, perform the following steps:

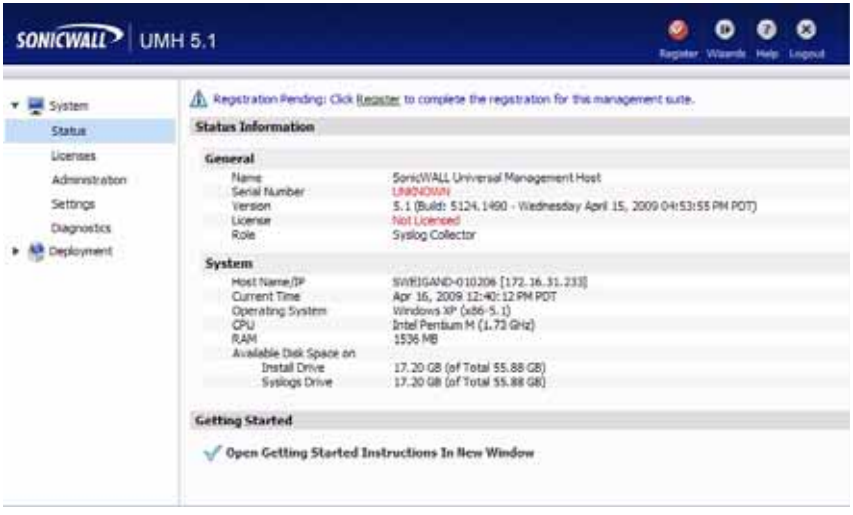
1. In a browser, log in to the system management interface (**http://**<*host*>**:80/appliance/login)**. If this is the first time you have logged in after running the Installer and rebooting, you will be required to change the password for the admin account. Enter the new password in the appropriate fields and then click **Submit**.

2. If the software detects that the Windows Firewall is enabled on the system, a warning dialog box is displayed on top of the System > Status page. To receive syslog and SNMP packets, either disable the Windows Firewall or configure it to open these ports (default syslog port UDP 514 and default SNMP port UDP 162). When ready, click **OK**.

   Optionally, you can select the **Perform this check after 30 days** checkbox if you do not plan to disable the Windows Firewall immediately, and do not wish to see this warning every time you login. The check for Windows Firewall cannot be disabled completely, and if you leave it running you will see this alert after the 30-day delay. You can repeat the delay as many times as needed.


Windows Firewall - Alert!
Please check Windows Firewall settings on the GMS/ViewPoint Server.
If Windows Firewall is enabled on your server, Syslog and SNMP packets will not be collected by the product, which will affect the Management, Alerting and Reporting functionalities of the product.
Please open 'Windows Firewall' in Control Panel to check the status of Windows Firewall. Make sure you have either disabled Windows Firewall software on the Server, or unblocked Syslog (typically UDP 514) and SNMP (UDP 162) packets.
Click OK only after you have undertaken these steps.
Perform this check after 30 days.
OK

3. In the System > Status page, click the **Register** button.



4. In the License Management page, type your MySonicWALL user name and password and then click **Submit**.

SONICWALL
UMH 5.1
Register
Wizards
Help
Logout
System
Status
Licenses
Administration
Settings
Diagnostics
Deployment
License Management
Serial Number: None
mySonicWALL.com Login
mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one.
Please enter your existing mySonicWALL.com username (or email address) and password below:
Email Address/User Name:
Password:
Submit
Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

5. In the next License Management page, type **VIEWPOINT** (all capital letters) into the **Serial Number** field and leave the **Authentication Code** fields blank. Type a descriptive name for the system into the **Friendly Name** field and then click **Submit**.

License Management
Serial Number: None
Enter your 12 character Software Serial Number, Authentication Code and a Friendly Name
For ViewPoint: Enter VIEWPOINT as Serial Number and ignore Authentication Code
Click here if you have an 8 character Serial Number
Serial Number:
Authentication Code:
What is this?
Friendly Name:
Submit

Note The Friendly Name for this system will also be used as the name for the SonicWALL ViewPoint deployment. As you register SonicWALL appliances on MySonicWALL, you will have the option of adding them to this deployment for SonicWALL ViewPoint reporting.

6. In the next License Management page, click **Continue**. This completes the registration process.

When registration is complete, the Deployment > Roles page is displayed. Although there is only one possible role for a SonicWALL ViewPoint deployment, you must still configure certain fields on this page and then click **Update** to fully activate the application. For instructions on configuring these settings, see the "Configuring the Deployment Role" section on page 32.

Configuring Deployment Settings

This section describes the settings available on the **Deployment > Settings** page of the UMH system management interface, available by default at:
http://localhost/appliance

Configuring Web Port Settings

To change the Web port settings, perform the following steps:

1. On the **Deployment > Settings** page under **Web Port Configuration**, to use a different port for HTTP access to the SonicWALL ViewPoint, type the port number into the **HTTP Port** field. The default port is 80.

2. To use a different port for HTTPS access to the SonicWALL ViewPoint, type the port number into the **HTTPS Port** field. The default port is 443.
3. Click **Update** to apply the Web port settings.

Note Changing the Web port settings will cause the system to restart.

4. After the appliance restarts, use the new port to access the "appliance" or SonicWALL ViewPoint management interface. For example:
   - If you changed the HTTP port to 8080, use the URL: **http://**<*IP Address*>**:8080/appliance/**
   - If you changed the HTTPS port to 4430, use the URL: **http://**<*IP Address*>**:4430/appliance/**

Configuring SMTP Settings

The SMTP settings are used for sending email alerts to the SonicWALL ViewPoint administrator. To configure the SMTP settings, perform the following steps:

1. On the **Deployment > Settings** page under **SMTP Configuration**, enter the IP address of the SMTP server into the **SMTP server** field.

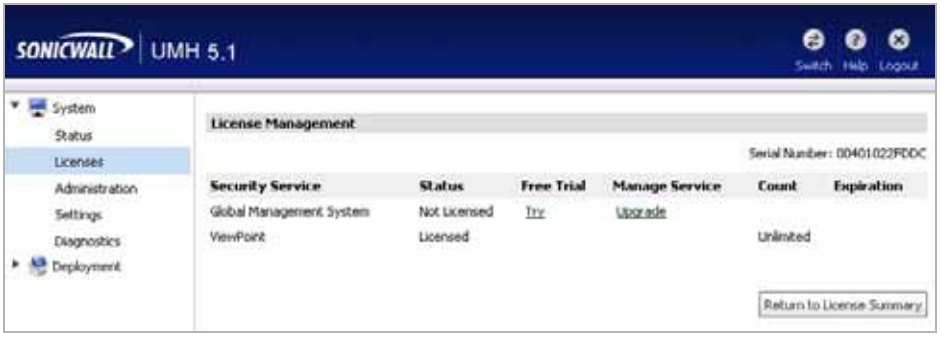
2. In the **Sender address** field, enter the email address that will appear as the 'From' address when email alerts are sent to the administrator.
3. In the **Administrator address** field, enter a valid email address for the administrator who will receive email alerts.
4. Click **Update** to apply the SMTP settings.

Upgrading from ViewPoint to GMS

SonicWALL ViewPoint installations have the option of upgrading to SonicWALL GMS without reinstalling. You can start a 30-day Free Trial of SonicWALL GMS by clicking a button or link in either the ViewPoint or Universal Management Host interface and following a simple procedure. When you are ready to finalize the upgrade, your SonicWALL reseller can provide you with the license key for a seamless transition to SonicWALL GMS.

When five or more registered devices are connected to SonicWALL ViewPoint reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL ViewPoint management interface.

You can also start the Free Trial by clicking **Manage Licenses** on the **System > Licenses** page of the Universal Management Host interface, and then clicking the **Try** link.



For details on enabling the SonicWALL GMS Free Trial and purchasing the SonicWALL GMS upgrade license, see the following sections:

- "Enabling the GMS Free Trial from ViewPoint" section on page 357
- "Enabling the GMS Free Trial from the UMH Interface" section on page 359
- "Completing the Free Trial Upgrade" section on page 360
- "Configuring Appliances for GMS Management" section on page 364
- "Purchasing a SonicWALL GMS Upgrade" section on page 366

Enabling the GMS Free Trial from ViewPoint

When five or more devices are connected to SonicWALL ViewPoint reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL ViewPoint management interface.

To find out how many devices your SonicWALL ViewPoint installation is handling, log in to MySonicWALL and navigate to the **My Products** page. Click on the link for your SonicWALL ViewPoint installation to get to the **Service Management** page, and scroll to the bottom. You will see the list of appliances under **Associated Products**.

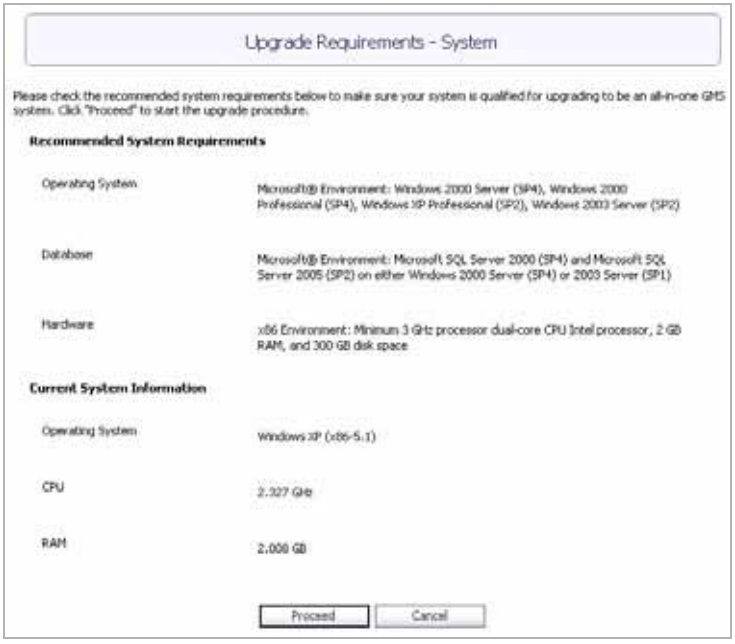
To enable the 30-day SonicWALL GMS Free Trial from the SonicWALL ViewPoint management interface, perform the following steps:

1. In the SonicWALL ViewPoint management interface, click the **Try GMS Free - 30 Days** button next to the tabs at the top of the page.

2. The Viewpoint Upgrade Tool launches and guides you through the process of installing the Free Trial or Upgrade. The tool displays the **Upgrade Requirements – Licensing** screen. Before migrating to GMS 5.1, ensure that all appliances under Viewpoint reporting are registered to the same MySonicWALL account. Follow the steps provided in the screen, and then click **Proceed**.

Upgrade Requirements - Licensing
ViewPoint to GMS 5.1 upgrade (GMS Free Trial or Full License), requires that all appliances in your ViewPoint software be registered to the same MySonicWALL account. If appliances are not migrated prior to this upgrade, GMS will be missing essential functionality such as the ability to license services and perform firmware upgrades. If this is the case, please abort the upgrade and consolidate all the appliances in your ViewPoint software into the same MySonicWALL account following the steps below. Otherwise, click "Proceed" to continue.
1. Gather the MySonicWALL login info for the appliance and log into the account.
2. After logging into MySonicWALL, navigate to the "My Products" screen and locate the appliance.
Important: Make note of the serial number and authentication code for future reference.
3. Locate the "delete" button option in the "Service Management" screen in the specific MySonicWALL account and select it.
4. Click on "Confirm Deletion" prompt.
5. This appliance is now ready for migration to GMS 5.1.
6. Repeat steps 1 thru 4 for the rest of the appliances under ViewPoint as needed.
Proceed
Cancel

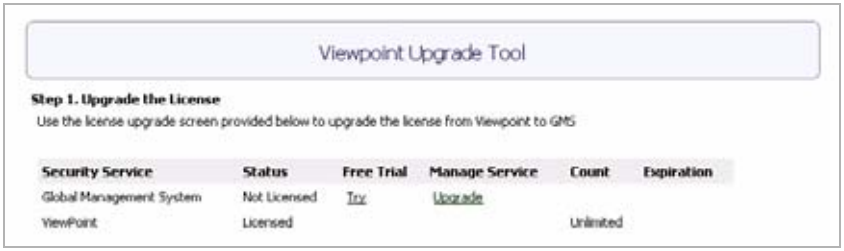
3. The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.


Upgrade Requirements - System
Please check the recommended system requirements below to make sure your system is qualified for upgrading to be an all-in-one GMS system. Click "Proceed" to start the upgrade procedure.
Recommended System Requirements
Operating System
Microsoft® Environment: Windows 2000 Server (SP4), Windows 2000 Professional (SP4), Windows XP Professional (SP2), Windows 2003 Server (SP2)
Database
Microsoft® Environment: Microsoft SQL Server 2000 (SP4) and Microsoft SQL Server 2005 (SP2) on either Windows 2000 Server (SP4) or 2003 Server (SP1)
Hardware
x86 Environment: Minimum 3 GHz processor dual-core CPU Intel processor, 2 GB RAM, and 300 GB disk space
Current System Information
Operating System
Windows XP (x86-5.1)
CPU
2.327 GHz
RAM
2.000 GB
Proceed
Cancel

4. The ViewPoint Upgrade Tool displays the login screen for MySonicWALL. Enter your MySonicWALL credentials and click **Submit**.

ViewPoint Upgrade Tool
Step 1. Upgrade the License
Use the license upgrade screen provided below to upgrade the license from Viewpoint to GMS
mySonicWALL.com Login
mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one.
Please enter your existing mySonicWALL.com username (or email address) and password below:
Email Address/User Name:
Password:
Submit
Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

5. In the next ViewPoint Upgrade Tool page, click the **Try** link in the **Free Trial** column for Global Management System.



6. From this point, the upgrade process continues with the same steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To continue the procedure, perform the steps in the "Completing the Free Trial Upgrade" section on page 360.

Enabling the GMS Free Trial from the UMH Interface

To enable the 30-day Free Trial of SonicWALL GMS from the Universal Management Host interface on your SonicWALL ViewPoint system, perform the following steps:

1. In the Universal Management Host interface, navigate to the System > Licenses page and click **Manage Licenses**.

2. If you are not already logged into MySonicWALL, the MySonicWALL login screen is displayed. Enter your MySonicWALL credentials in the appropriate fields and log in.

3. On the next page, click the **Try** link in the **Free Trial** column for Global Management System.

4. From this point, the upgrade process continues with the same steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To continue the procedure, perform the steps in the "Completing the Free Trial Upgrade" section on page 360.

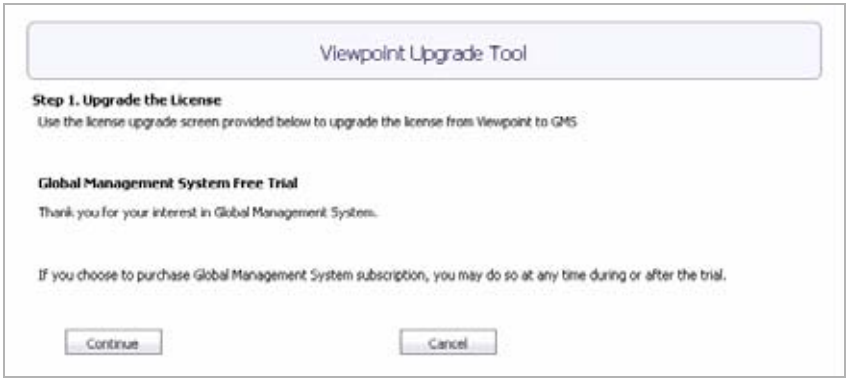
Completing the Free Trial Upgrade

This procedure provides the common upgrading steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To get to this point in the process, follow the steps described in one of the two preceding sections:

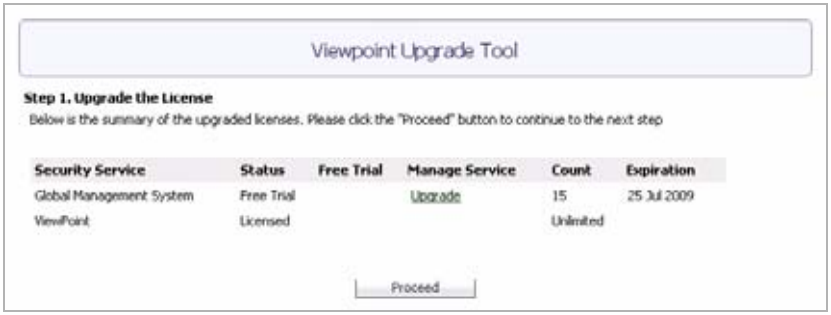
- "Enabling the GMS Free Trial from ViewPoint" section on page 357
- "Enabling the GMS Free Trial from the UMH Interface" section on page 359

To continue the upgrade, perform the following steps:

1. In the ViewPoint Upgrade Tool page, click the **Continue** button.


Viewpoint Upgrade Tool
Step 1. Upgrade the License
Use the license upgrade screen provided below to upgrade the license from Viewpoint to GMS
Global Management System Free Trial
Thank you for your interest in Global Management System.
If you choose to purchase Global Management System subscription, you may do so at any time during or after the trial.
Continue
Cancel

2. The next screen provides a summary of GMS and ViewPoint status. Verify that the **Try** link for the Free Trial is gone and only the **Upgrade** link remains. The **Expiration** column displays the expiration date of your Free Trial. You can click the **Upgrade** link at any time during the Free Trial to purchase the SonicWALL GMS upgrade. Click **Proceed**.



3. In the next ViewPoint Upgrade Tool page, you begin the configuration for SonicWALL GMS instep 2 of the upgrade process. This page displays two sections:

   Automatic Configuration – Contains a list of SonicWALL UTM or CSM appliances in your ViewPoint installation. These appliances will be automatically configured for SonicWALL GMS management.

   Manual Configuration – Contains a list of SonicWALL Aventail, SSL-VPN, or CDP appliances in your ViewPoint installation. You must manually configure these appliances for SonicWALL GMS management. See the "Configuring Appliances for GMS Management" section on page 364 for detailed instructions on enabling SonicWALL GMS management on these appliances.

When ready, click **Proceed**.

ViewPoint Upgrade Tool
Automatic Configuration
Following list shows all the UTM appliances currently in the system. These appliances can be automatically configured to support GMS .
Appliance Name
Appliance Serial Number
NSA 240
0017C5269510
NSA 5500
0017C51C655C
Manual Configuration
Following list shows all the non-UTM appliances currently in the system. These appliances need manual configuration to support GMS .
Appliance Name
Appliance Serial
Eng Test
0006B1275C34

4. When the configuration finishes, the ViewPoint Upgrade Tool displays the completion dialog box. Click **Close** to log out of the console and restart the system.

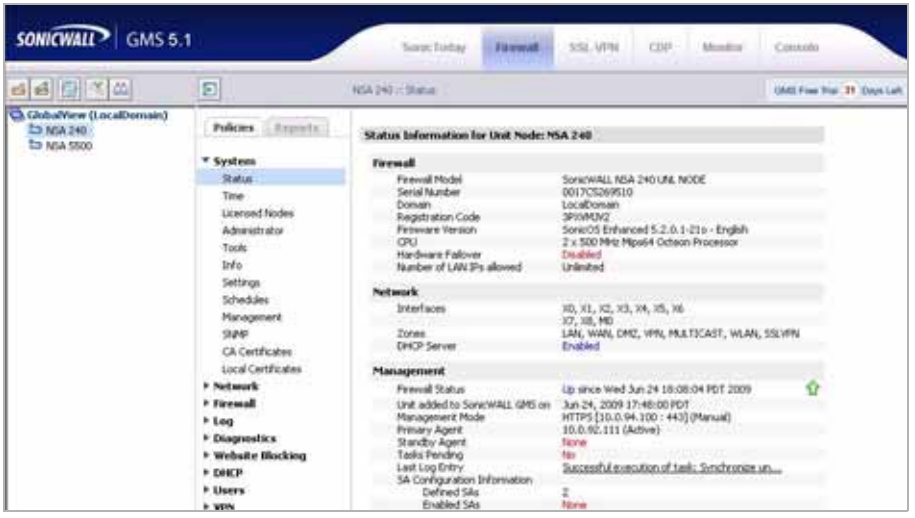
Viewpoint Upgrade Tool
You have complete the upgrade procedure.
please click "Close" button to logout the console and reboot the box
close
SONICWALL

5. The GMS login page appears and requests that you reboot the system. Reboot the system. If a reboot is not performed, you may encounter problems with the correct IP Address appearing.

6. After rebooting, log in with your ViewPoint credentials.

   When you log in, you will see a button displaying the number of days left in your Free Trial at the top of the page.

7. On the System > Status page for connected appliances, you can view the log entries for task synchronization and automatic addressing mode, related to the GMS configuration.



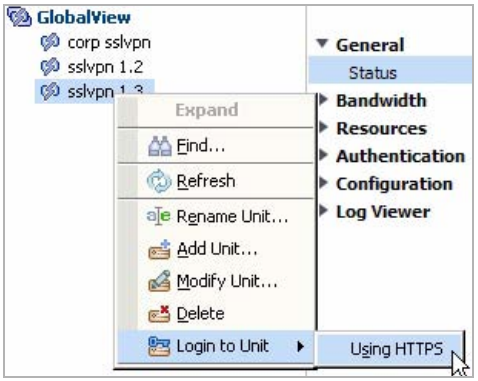
Configuring Appliances for GMS Management

To manually configure the appliances listed in the Manual Configuration section of the ViewPoint Upgrade Tool page (see Step 3. on page 361), perform the following steps for each appliance:

1. In the SonicWALL GMS management interface, click the tab at the top of the page that corresponds to the type of appliance, such as **SSL-VPN** or **CDP**.
2. In the left pane, right-click one of the listed appliances and select **Modify Unit**.
3. In the Modify Unit screen in the right pane, copy the appliance IP address in the **Managed Address** section to your clipboard, or make a note of it.

4. Click **Cancel**.

5. In the left pane, right-click the same appliance and select **Login to Unit > Using HTTPS**.



6. In the appliance management interface, navigate to the System > Administration page.

7. Under **GMS Settings**, select the **Enable GMS Management** checkbox, or verify that it is selected.
8. In the **GMS Host Name or IP Address** field, paste or type the appliance IP address that you obtained from the Modify Unit screen in Step 3.
9. Click the **Accept** button at the top of the appliance interface screen.
10. Click the **Logout** button in the top right corner of the appliance interface screen.
11. Repeat these steps for each appliance listed in the Manual Configuration section of the ViewPoint Upgrade Tool page.

Purchasing a SonicWALL GMS Upgrade

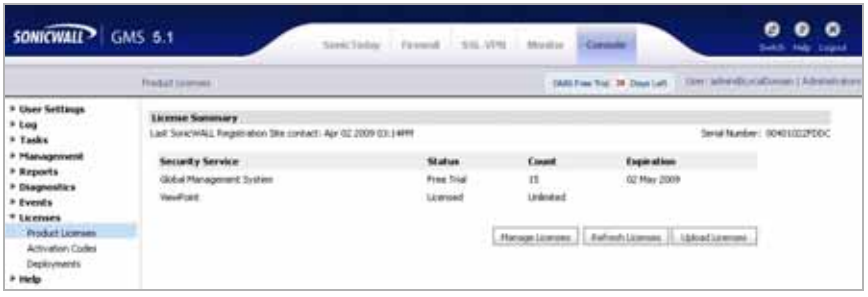
You can purchase an upgrade to SonicWALL GMS at any time during the 30-day Free Trial.

To purchase the SonicWALL GMS license, perform the following steps:

1. In the SonicWALL GMS interface, click the **GMS Free Trial X Days Left** button, where X is the number of days left in the Free Trial.

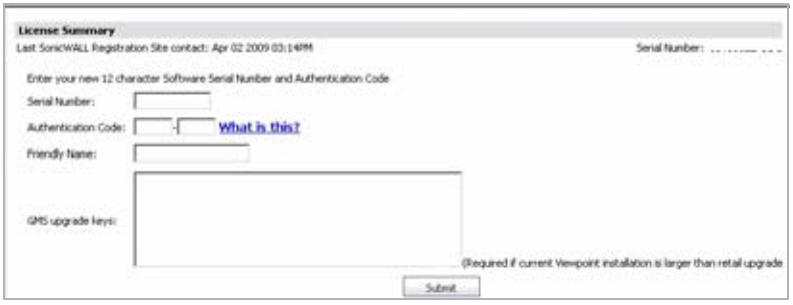
2. In the **Buy GMS** page, click **I want to upgrade to GMS now**.

3. The Console > Licenses > Product Licenses page is displayed. Click **Manage Licenses**.



4. In the next page, in the **Manage Service** column for Global Management System, click the **Upgrade** link.

5. The next page has **Serial Number** and **Authentication Code** fields for SonicWALL GMS. You must contact your SonicWALL reseller to complete the purchase and obtain the 12-character serial number and authentication code. Type in the values to the **Serial Number** and **Authentication Code** fields.


License Summary
Last SonicWALL Registration Site contact: Apr 02 2009 03:14PM
Serial Number:
Enter your new 12 character Software Serial Number and Authentication Code
Serial Number:
Authentication Code:
What is this?
Friendly Name:
GMS upgrade keys:
(Required if current Viewpoint installation is larger than retail upgrade
Submit

6. Enter a descriptive name for the SonicWALL GMS installation into the **Friendly Name** field. This name will appear in your MySonicWALL account.

7. If your SonicWALL ViewPoint installation currently handles more than 10 appliances, when you upgrade to SonicWALL GMS you will need to purchase additional SonicWALL GMS license(s) to manage the extra appliances. The standard "10-node" SonicWALL GMS license provided with the Free Trial supports up to 10 managed appliances. Enter the license keys for any additional SonicWALL GMS licenses into the **GMS upgrade keys** text box, one key per line.

8. Click **Submit**. The License page is displayed, showing that SonicWALL GMS is now licensed.

Miscellaneous Procedures and Troubleshooting Tips

This section contains miscellaneous SonicWALL ViewPoint procedures and troubleshooting tips.

Miscellaneous Procedures

This section contains information on procedures that you may need to perform. Select from the following:

- It is highly recommended that you regularly back up the SonicWALL ViewPoint data. For more information, see "Backing up SonicWALL ViewPoint Data" on page 368.
- SonicWALL ViewPoint requires Mixed Mode authentication when using SQL Server 2000. To change the authentication mode, see "Changing the SQL Server Authentication Mode" on page 369.
- If you are reinstalling SonicWALL ViewPoint, preserving the previous configuration settings can save a lot of time. To reinstall SonicWALL ViewPoint using an existing SonicWALL ViewPoint database, see "Reinstalling SonicWALL ViewPoint Using an Existing Database" on page 369.
- If you need to uninstall SonicWALL ViewPoint from a server, it is important to do it correctly. To uninstall SonicWALL ViewPoint, see "Uninstalling SonicWALL Universal Management Suite and Its Database" on page 369.

Backing up SonicWALL ViewPoint Data

SonicWALL ViewPoint stores its configuration data in the SGMSDB database. It is important to back up this database and the individual SonicWALL ViewPoint databases (sgmsvp_yyyy_mm_dd) on a regular basis.

The Console > Management > Database Maintenance page provides the necessary support for backing up and restoring the MySQL database that is bundled with SonicWALL UMS. For more information, see the "Database Maintenance" section on page 66.

If you are using SQL Server, this can be accomplished by backing up the entire SQL Server using the database backup tool. When using this tool, there is no need to stop the SonicWALL ViewPoint services for database backup. However, make sure that the backup occurs when SonicWALL ViewPoint activity is the lowest and that the backup operation schedule does not clash with the SonicWALL ViewPoint scheduler.

Note It is also recommended to regularly back up the entire contents of the SonicWALL ViewPoint directory, the sgmsConfig.xml file.

Changing the SQL Server Authentication Mode

SonicWALL ViewPoint requires the Mixed Mode authentication mode. To change the authentication mode from Windows Mode to Mixed Mode, follow these steps:

1. Start the Microsoft SQL Server Enterprise Manager.
2. Right-click the appropriate SQL Server Group and select **Properties** from the pop-up menu.
3. Click the **Security** tab.
4. Change the Authentication mode from **Windows only** to **SQL Server and Windows**.
5. Click **OK**.

Reinstalling SonicWALL ViewPoint Using an Existing Database

If you need to reinstall SonicWALL ViewPoint, but want to preserve the settings in an existing SonicWALL ViewPoint database, follow these steps:

1. Install a new database, using the same username and password that you used for the existing SonicWALL ViewPoint database.
2. Install SonicWALL ViewPoint using this new database.
3. Stop all SonicWALL ViewPoint services.
4. Open the sgmsConfig.xml and web.xml files with a text editor. Change the values for the dbhost and dburl parameters to match the existing SonicWALL ViewPoint database.
5. Restart the SonicWALL ViewPoint services.
6. Uninstall the new database.

Uninstalling SonicWALL Universal Management Suite and Its Database

This section describes how to uninstall SonicWALL Universal Management Suite and its components. Select from the following:

- To uninstall SonicWALL Universal Management Suite on the Windows platform, see “Windows” on page 370.

- To uninstall SonicWALL Universal Management Suite databases from Microsoft SQL Server 2000, see "MS SQL Server 2000" on page 370.

Windows

To uninstall SonicWALL Universal Management Suite from a Windows system, follow these steps:

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs Properties window displays.
3. Select **SonicWALL Universal Management Suite** and click **Change/Remove**. The SonicWALL Universal Management Suite Uninstall program starts.
4. Follow the on-screen prompts.
5. Restart the system. SonicWALL Universal Management Suite is uninstalled.

MS SQL Server 2000

To uninstall or remove the SonicWALL Universal Management Suite databases in the MS SQL Server 2000, you can execute the following DOS command from any SonicWALL Universal Management Suite server:

```
osql -U username -P password -S dbHost_IP -q "drop database SGMSDB"
osql -U username -P password -S dbHost_IP -q "drop database sgmsvp_yyyy_mm_dd"
```

Or you can use the MS SQL Server's Enterprise Manager and delete the SGMSDB and sgmsvp_ databases.

Troubleshooting Tips

This section contains SonicWALL ViewPoint troubleshooting tips.

Changing the Default Syslog Server Port Number

By default, the SonicWALL ViewPoint syslog server default port number is 514 on Windows systems. To change the port number, follow these steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Add the following line to the end of the file before the </Configuration> section:

Parameter name="syslog.syslogServerPort" value="*port_number*"

where *port_number* is the new port number.

3. Save the file and exit.

Installing the Java Plug In

You need Java Plug-in 1.6 or later to access the SonicWALL ViewPoint management interface.

Tip The Java Plug-in is automatically installed during the SonicWALL ViewPoint installation. However, you can manually install the Java Plug-in by following these steps.

To manually install the Java Plug-in, perform the following steps:

1. Download the installer from the Internet at:

   http://java.sun.com/javase/downloads/index.jsp

Here are the Java SE downloads in detail.
Java SE Development Kit (JDK)
JDK 6 Update 17
The JDK (which includes the JRE) is required to develop Java and JavaFX applications and applets. This special release provides a few key fixes.
» Learn more
Due for release in November 2009, the Firefox 3.6 browser requires Java SE 6 Update 10 or later. Otherwise, Java-based web applications will not work.
Download
Docs
Java SE Runtime Environment (JRE)
JRE 6 Update 17
The JRE is required to run Java and JavaFX applications and applets. This special release provides a few key fixes. » Learn more
Due for release in November 2009, the Firefox 3.6 browser requires Java SE 6 Update 10 or later. Otherwise, Java-based web applications will not work.
Download
Docs

2. Execute the installer.
3. Select the radio button next to **Accept the Terms of the License Agreement**. Click **Next**.
4. Select the radio button next to **Typical** installation and click **Next**.
5. It may take several minutes for the Java Plug-in to install.
6. In the Installation Complete window, click **Finish**.
   - Restart your computer to complete the installation process.

Appendix B

Technical Tips

This chapter includes the following sections:

- "Log Viewer" section on page 373
- "Real-time Syslog Viewer" section on page 375
- "Forwarding Syslog Data to Another Syslog Server" section on page 376
- "Posting ViewPoint Reporting to Another Web Server for End-User Access" section on page 377

Log Viewer

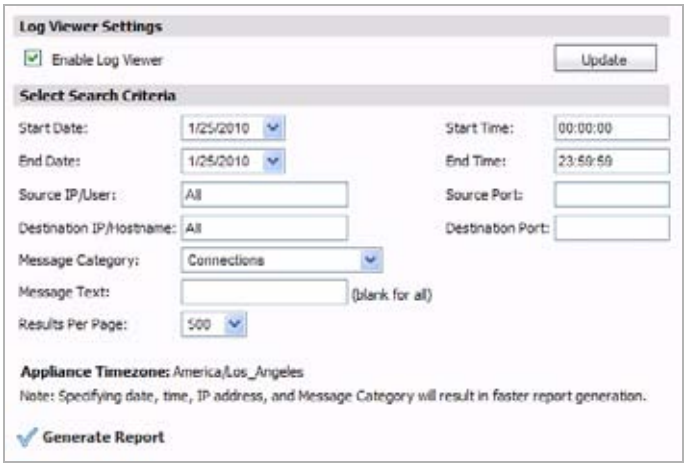
The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance. This information is stored for the time that you specified in the configuration settings.

Note The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For information about setting the number of days data is stored, see "Enabling Report Table Sorting" on page 72.

To configure Log Viewer settings for generating a report, perform the following steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **UTM** or **SSL-VPN** tab.

3. Select a SonicWALL appliance.
4. Expand the **Log Viewer** tree and click **Search**. The Search page displays. Log Viewer must be enabled for the appliance in order to display all the fields on the page.

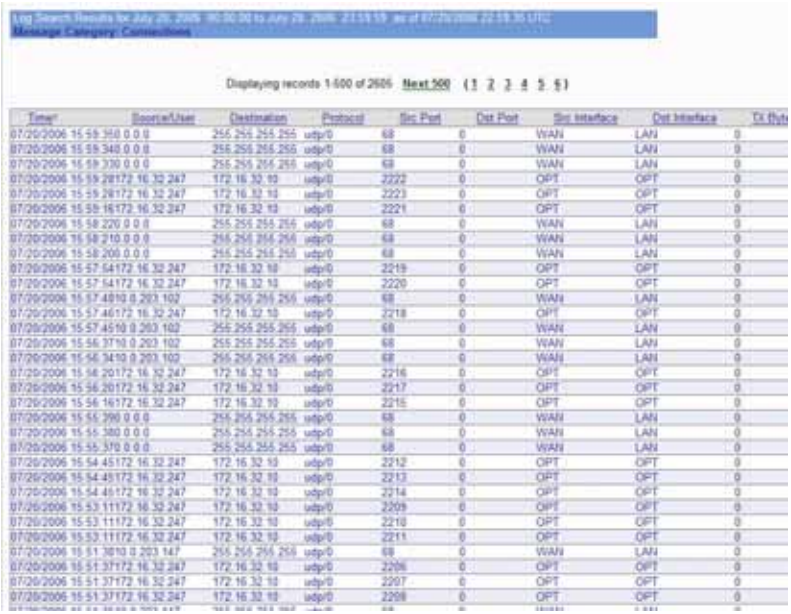


5. Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer. The maximum number of appliances for which Log Viewer can be enabled is controlled on the Console > Reports > Settings page. See "Controlling the Number of Appliances with Log Viewer Enabled" on page 72.

Note Custom Reports are available on appliances with Log Viewer enabled. See "Using Custom Reports on UTM Appliances" on page 163.

6. Select the starting date to view from the **Start Date** list box.
7. Enter the starting time of events to view in the **Start Time** field.
8. Select the ending date of events to view in the **End Date** list box
9. Enter the ending time of events to view in the **End Time** field.
10. Enter the source IP address to view in the **Source IP Address** field. To view all IP addresses, enter All.
11. Optionally enter the source port to view in the **Source Port** field.
12. Enter the destination IP address to view in the **Destination IP Address** field. To view all IP addresses, enter All.

13. Optionally enter the destination port to view in the **Destination Port** field.
14. Select the type of events to view from the **Message Category** list box.
15. To search for specific message text, type the text into the **Message Text** field.
16. Select the number of entries to display per page from the **Results Per Page** field.
17. Click **Generate Report**. The Log Viewer Results page displays.



Real-time Syslog Viewer

The real-time syslog utility enables you to diagnose the system by viewing the syslog messages in real time.

Note Only use this utility when needed for diagnostic purposes.

To open the real-time syslog utility, perform the following steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **UTM** or **SSL-VPN** tab.
3. Expand **Real-Time Viewer** and click **Syslog**. The Real-Time Syslog page appears.
4. If syslog forwarding is not enabled, select **Enable Syslog Forwarding**, set the IP address and port used by the syslog reader, and then click **Update**.

5. If the Syslog Reader is not already running, click **Start Syslog Reader**.
6. Click **Start Button** at the bottom of the screen. The Syslog Viewer begins showing the latest syslog entries.

Syslog Reader Configuration
Enable Syslog Forwarding
IP Address: 127.0.0.1
Port: 21007
Update
Reset
Note:
* The IP Address specified should be the Console/Web Server IP address.
(Recommended value for port is 21007).
* It may take a few minutes for the system to update the new configuration.
Start Syslog Reader
Current Status
Syslog forwarding is enabled (IP Address: 127.0.0.1, Port:21007)
DOCK
Syslog Reader is currently NOT running.
Please start the Syslog Reader.
(Note:If you do not have sufficient privileges, please contact the administrator).

7. To change how many messages are displayed, select a number from the **Number of Messages** list box at the bottom of the screen.

8. To change how often the Syslog Viewer is refreshed, select the time from the **Refresh Time** list box at the bottom of the screen.
9. To stop the viewer, click the **Stop** button.
10. To search for text, use the browser's Find utility.
11. When you are finished, close the Syslog Viewer.

Forwarding Syslog Data to Another Syslog Server

To forward SonicWALL ViewPoint syslog data to another syslog server, perform the following steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Locate the following line:

   Parameter name =“syslog.forwardToHost” value=“”
3. Add the IP address or hostname of the destination syslog server to the value attribute.
4. Save the sgmsConfig.xml file and exit.

5. Ensure that at least firmware 6.3.1.0 is running on the SonicWALL appliances.

Note To configure SonicWALL ViewPoint to not store the syslog data after it has been forwarded, you must disable the ViewPoint Reporting Module. To do this, open the ViewPoint **Settings** page in the Console Panel, deselect the **Enable Reporting** check box, and click **Update**.

Posting ViewPoint Reporting to Another Web Server for End-User Access

To allow end user access to another web server for end-user access, install the SonicWALL ViewPoint Console in redundant mode.

You can then allow end user access to the redundant Console for viewing ViewPoint Reporting real-time and historical reports. End user access will be isolated from the main Console that is used for managing and configuring SonicWALL appliances.

Index

A

activating
ViewPoint 341
alert types 100
alerting
using GEM 97
anti-spyware
reports 266
applets
signed 21
Application Firewall reports 281
archive
in Console>Reports 132
MDTA 87
on Console>Reports 81
report settings 81
scheduled report 135
summarizer data 87
Attacks reports 250
authentication code 353
Authentication reports 287

B

Bandwidth reports 180
benefits
of compliance reports 144
of report data management 87
of SSL VPN reporting 294
browser
requirements 338

C

Compliance reports
configuration 152
overview 144
compliance reports 144
console
management settings 61
cover page
customizing 147
Custom Reports
Resource Activity 307
customizing
detailed report 149
report cover page 147
summary report 148

D

dashboard 159
Dashboard Summary report 159
data
management 87
database
backing up 368
reinstalling with existing db 369
requirements 337

deployment
settings 354
detailed report
customizing 149
digital
signature in applet 21
disabling
GEM thresholds 103
domain names
in reports 130

E

email
report settings 81
enabling
GEM thresholds 103
report table sorting 71
events
GEM overview 97
schedules 98
severities 97
thresholds 98

F

File Transfer Protocol
See FTP
free trial
for GMS 356
for GMS, configuring appliances 364
for GMS, enabling from UMH interface 359
for GMS, enabling from ViewPoint 357
friendly name 353
FTP reports 225

G

GEM
alert types 100
configuring 101
default settings 99
overview 97, 98
schedules 98
severites 97
thresholds 98
global view 117
global views 120
GMS
upgrading to from ViewPoint 356
Granular Event Management
See GEM

H

hardware
requirements 339
help
viewing online help 24
host name resolution 79

I

inheritance
report settings 138

installing
appendix 335
appliance, firmware support 339
browser requirements 338
database requirements 337
deployment settings 354
hardware requirements 339
Java requirements 338
network requirements 339
on Windows 342
overview 10
system requirements 337
task list 336
Universal Management Suite 342
interfaces
accessing both 11
overview of ViewPoint application 13
switching between 12, 24
TreeControl 20
UMH deployment options 31
UMH deployment role 32
UMH deployment services 36
UMH HTTP(S) settings 34
UMH SMTP settings 34
UMH system administration 28
UMH system diagnostics 30
UMH system interface overview 24
UMH system licenses 26
UMH system settings 25
UMH system software 29
UMH system status 26
IPS
reports 273

J

Java
plugin 371
requirements 338
java.policy file 21

L

licensing
requirements 10
SonicWALL appliances for use with ViewPoint 10
ViewPoint on appliances 342
log
viewing 58
Log Viewer 290, 332
log viewer
for SSL VPN appliances 332
logging out 25

M

Mail Usage reports 231
MDTA 87
MySonicWALL
creating an account 340

N

name resolution crawler 79
network
requirements 339

P

pagination
settings 51
password
settings 51
PDF
exporting reports to 144
reports 152
port
syslog 370
profiles
existing 150
scheduled report 149

R

registering
- procedure 351
- requirements 10
- SonicWALL appliances 341

reporting
- overview 115
- search bar 116, 118

reports
- adding scheduled 135
- Browse Time 128
- By Site to By User navigation 129
- compliance 144
- cover pages 147
- domains or IP addresses 130
- inheritance 138
- no data 156
- PDF format 144
- ROI 128
- searching by dates of 155
- settings 154
- SSL VPN 295
- SSL VPN authentication 330
- SSL VPN bandwidth 301
- SSL VPN custom resource activity 307
- SSL VPN overview 293
- SSL VPN resources 325
- SSL VPN scheduled reports 296
- SSL VPN summarization 297
- viewing Dashboard 159
- views 17
- Web usage, exclusions 53

requirements
- browser 338
- database 337
- hardware 339
- Java 338
- network 339
- system 337

reverse inheritance
- for reporting 139

role
- configuring 32

S

scheduled reports
- disabling/enabling 128

scheduler
- link to from report page 118

schedules 98
- resending 86

search bar 116, 118
- components of 123
- operators 125

Security Dashboard reports 159
serial number 353
- GMS 114

services
- enabling/disabling 36

Services reports 189
sessions
- managing 65

settings
- inactivity timeout 51
- pagination 51
- password 51
- website exclusion list 53

severities 97
signed applets 21
SMTP
- settings 34, 355

SNMP
port 339
SQL
authentication mode 369
status
viewing 17
summarizer
configuring reports to create 137
instant summary reports 76
using Summarize Now 76
summary report
customizing 148
syslog
port 339
port number 370
system
requirements 337
system interface
deployment options 31
deployment role 32
deployment services 36
HTTP(S) settings 34
overview 24
SMTP settings 34
system administration 28
system diagnostics 30
system licenses 26
system settings 25
system software 29
system status 26

T

thresholds 98
timeout
inactivity settings 51
TreeControl
collapsing/hiding the pane 20, 128
menu 20
troubleshooting 368, 370
reports, no data 156

U

UMH interface
deployment options 31
deployment role 32
deployment services 36
HTTP(S) settings 34
overview 24
SMTP settings 34
system administration 28
system diagnostics 30
system licenses 26
system settings 25
system software 29
system status 26
uninstalling 369
unit view 121
Universal Management Suite
installing 342
upgrading
purchasing GMS upgrade 366
upgrade key 336
ViewPoint to GMS 356
users
managing sessions 65
settings 51

V

views
global 120
unit 121
Virus Attacks Reports 260
VPN Usage reports 238

W

Web
port configuration 354
port settings 34

web event consolidation 141
Web Filter reports 209
Web usage
    exclusion list 53
Web Usage reports 191
Windows Firewall
    disabling 339, 352

SonicWALL, Inc.
2001 Logic Drive
San Jose CA 95124-3452
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

PN: 232-001802-00 Rev A 3/2010

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.